IP-Reach

Benutzer-handbuch

IPR-TR361
IPR-TR362
IPR-TR364
IPR-M1
IPR-M2
Version 3.2

Raritan Computer Inc.
400 Cottontail Lane
Somerset, NJ 08873, USA
USA
Tel.: 732-764-8886
Fax: 732-764-8887
E-Mail: sales@raritan.com
http://www.raritan.com

Raritan Computer Japan, Inc.
4th Flr. Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku,
Tokyo 104-0033
Japan
Tel.: 81-03-3523-5991
Fax: 81-03-3523-5992
E-Mail: sales@raritan.co.jp
http://www.raritan.co.jp

Raritan Computer Frankreich
120 Rue Jean Jaurès
93200 Levallois-Perret
France
Tel.: 33-14-756-2039
Fax: 33-14-756-2061
E-Mail: sales.france@raritan.com
http://www.raritan.fr

Raritan Computer U.K. Ltd.
36 Great St. Helen's
London
EC3A 6AP
United Kingdom
Tel.: 44 20 7614 7700
Fax: 44 20 7614 7701
E-Mail: sales.uk@raritan.com
http://www.raritan.com

Raritan Computer Europe B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel.: 31-10-284-4040
Fax: 31-10-284-4049
E-Mail: sales.europe@raritan.com
http://www.raritan.com

Raritan Computer Taiwan, Inc.
5F, 121, Lane 235,
Pao-Chiao Rd., Hsin Tien
Taipei Hsien
Taiwan, ROC
Tel.: 886-2-8919-1333
Fax: 886-2-8919-1338
E-Mail: sales.asia@raritan.com
http://www.raritan.com.tw

Raritan Computer Deutschland GmbH
Lichtstraße 2
D-45127 Essen
Germany
Tel.: 49-201-747-9820
Fax: 49-201-747-9850
E-Mail: sales.germany@raritan.com
http://www.raritan.de

Raritan Computer, Inc.
Vertretung in Shanghai
RM 19C-1 Shanghai Shiye Building
18 Caoxi North Road
Shanghai China 2000030
Tel.: 86-21-64680475
Fax: 86-21-64627964
E-Mail: sales.asia@raritan.com
http://www.raritan.com.tw

CE c UL us LISTED 1F61 I.T.E.

Copyright © 2004 Raritan Computer, Inc.

IPR-0I-E
Juni 2004
255-80-3105

Raritan

FCC-Informationen

Dieses Gerät wurde getestet und entspricht den Beschränkungen für ein digitales Gerät der Klasse A gemäß Teil 15 der FCC-Richtlinien („Federal Communications Comission“, zuständig für die Überprüfung von Strahlungsstörungen bei elektronischen Geräten) in den USA. Diese Beschränkungen dienen dem Schutz vor schädlichen Interferenzstörungen in Heiminstallationen. Dieses Gerät erzeugt, verwendet und strahlt Energie im Radiofrequenzbereich aus. Wenn es nicht gemäß den Anweisungen installiert und verwendet wird, kann sein Betrieb schädliche Interferenzen im Funkverkehr verursachen. Der Betrieb dieses Geräts in einer Wohngegend kann schädliche Interferenzen verursachen.

Markenschutzinformationen

Die in diesem Handbuch aufgelisteten Produkte sind Marken oder eingetragene Marken der entsprechenden Firmen. IP-Reach, Paragon, MasterConsole MX[4], MasterConsole II, MasterConsole und die entsprechenden Logos sind Marken oder eingetragene Marken von Raritan Computer, Inc. PS/2, RS/6000 und PC/AT sind eingetragene Marken der International Business Machines Corporation. Sun ist eine eingetragene Marke von Sun Microsystems. Microsoft und Windows sind eingetragene Marken der Microsoft Corporation. Alle anderen Marken gehören den jeweiligen Unternehmen.

Japanische Zulassungen

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Unterstützung in den USA erhalten Sie vom technischen Kundendienst von Raritan unter der Telefonnummer (732) 764-8886, der Faxnummer (732) 764-8887 oder per E-Mail tech@raritan.com.

Der technische Kundendienst steht Ihnen von Montag bis Freitag zwischen 8.00 und 20.00 Uhr (Ortszeit) zur Verfügung.

Außerhalb der USA wenden Sie sich bitte an Ihre regionale Raritan-Niederlassung.

Diese Seite wurde absichtlich leer gelassen.

Inhalt

Kapitel 1: Einleitung 1

IP-Reach – Überblick 1
Zugriff über Internet, LAN/WAN oder DFÜ-Modem 1
Produktfotos 2
Paketinhalt 2
Produktfeatures 3
Terminologie 4
Modellreihen 4

Kapitel 2: Installation 5

Konfigurieren der Zielserver 5
Videoauflösung des Servers 5
Einstellungen für Windows XP 5
Einstellungen für Windows 2000/ME 5
Einstellungen für Windows 95/98/NT 6
Einstellungen für Linux 6
Einstellungen für Sun Solaris 6
Einstellungen für Apple Macintosh 6
Einstellungen für Apple Macintosh 7
Konfigurieren der Einstellungen für die Netzwerkfirewall 7
Konfigurieren von Paragon-KVM-Switches 7
Physische Anschlüsse der TR-Serie 8
Netzkabel 8
Lokale Verwaltungskonsole 8
Primärer Netzwerkport 8
Sekundärer Netzwerkport (optional) 8
KVM-Eingangsports 8
KVM-Ausgangsports/Ports der lokalen Zugriffskonsole (optional) 8
Telefonleitungsport (optional) 9
Serieller Eingangsport (optional) 9
Physische Anschlüsse der M-Serie 9
Netzkabel 9
Lokale Verwaltungskonsole 9
Netzwerkport 10
KVM-Eingangsports 10
KVM-Ausgangsports/Ports der lokalen Zugriffskonsole (optional) 10
Dedizierter Modemport (optional) 10
Serieller Eingangsport (optional) 10
Erstkonfiguration 12
Herstellen einer Remoteverbindung zu IP-Reach 14
Starten von Raritan Remote Client (RRC) 14
Einrichten einer Verbindung 15
Hinweis für CommandCenter-Benutzer 15

Kapitel 3: Raritan Remote Client 17

Aufrufen von Raritan Remote Client (RRC) über einen Webbrowser 17
Sicherheitseinstellungen 17
Starten von Raritan Remote Client 17
Entfernen von RRC aus dem Browsercache 18
Optional: Installieren von Raritan Remote Client-Software 19
RRC-Fensteranordnung 20
RRC-Navigator 21
Navigator-Optionen 22
Erstellen neuer Profile 22
Einrichten einer neuen Verbindung 24
Beenden einer Remoteverbindung 24
RRC-Symbolleiste und Verknüpfungen 25
RRC-Statusleiste 26
Remote-KVM-Konsolensteuerung 27
Ein-Cursor-Modus/Zwei-Cursor-Modus 28
Vollbildmodus 28
Auswählen von Servern anhand eines KVM-Switches 29
Tastaturmakros 30
Verbindungs- und Videoeigenschaften 33
Farbkalibrierung 36
Serielle Remotesteuerung 37
Physische Anschlüsse 37
Remoteverbindung 37
Ändern serieller Einstellungen 38

Remotegeräteadministration 38
Konfigurationsmenüs 38
Firmwareaktualisierung 38
Geräteneustart 38
Sicherung und Wiederherstellung der Gerätekonfiguration 38
Protokolldateien 39

Kapitel 4: Verwaltungsfunktionen 41

Zugriff auf die Verwaltungsfunktionen 41
Lokale Verwaltungskonsole 41
Remoteverwaltung 42
Navigieren in den Verwaltungsmenüs 42
Netzwerkkonfiguration 43
Path Configuration (Pfadkonfiguration) 44
Sicherheitskonfiguration 47
Leistungseinstellungen 49
Remoteauthentifizierung: Benutzer, Gruppen und Zugriffsberechtigungen 50
Überblick 50
Beziehung zwischen Benutzern und Gruppeneinträgen 51
Erstellen oder Ändern von Gruppenkonten 51
Zuweisen von Portzugriffsberechtigungen 53
Löschen von Gruppenkonten 54
Erstellen oder Ändern von Benutzerkonten 55
Benutzerkonten löschen 56
Implementierung der Remoteauthentifizierung 57
Einleitung 57
Implementierung der Remoteauthentifizierung 57
Allgemeine Einstellungen für die Remoteauthentifizierung 59
Uhrzeit und Datum 63
Abmelden von Benutzern 63
Anzeigen des IP-Reach-Status 64
Neustart oder Herunterfahren von IP-Reach 64
Diagnose 65

Anhang A: Technische Daten 67

Remoteverbindung 67
Raritan Remote Client (RRC)-Software 67
KVM-Eingabe 67
Kabelspezifikationen 68
KVM Switch-Spezifikationen 68
Ausgangsspezifikationen 68

Anhang B: SNMP-Funktionen 69

Anhang C: Häufig gestellte Fragen 71

Anhang D: Problembehandlung 75

Probleme und Lösungsvorschläge 75
Ereignisprotokolldatei und Bildschirmfehlercodes 80

Wichtige Informationen

Anmeldung

- Der Standardbenutzername für die IP-Reach-Anmeldung lautet <admin> und das Kennwort <raritan>. Dieser Benutzer besitzt Administratorrechte.
- Kennwörter unterliegen der Groß-/Kleinschreibung und müssen genau in der bei ihrer Erstellung verwendeten Schreibweise eingegeben werden.
- Das Standardkennwort <raritan> muss in Kleinbuchstaben eingegeben werden.
- Zur Gewährleistung der Sicherheit sollte das Standardkennwort so bald wie möglich geändert werden.

Standard-IP-Adresse

- IP-Reach wird mit der Standard-IP-Adresse 192.168.0.192 geliefert.

Firmware

- Dieses Handbuch bezieht sich auf IP-Reach Firmware Version 3.2 und höher.

TeleReach

- Bis zum 31. Januar 2003 war die IP-Reach-Produktlinie unter dem Namen „TeleReach“ bekannt.

Diese Seite wurde absichtlich leer gelassen.

Kapitel 1: Einleitung

IP-Reach – Überblick

Wir gratulieren zum Kauf von IP-Reach, der branchenführenden Lösung für plattformübergreifenden High-Performance- und netzwerkbasierten Remote-KVM-Konsolenzugriff. IP-Reach ermöglicht über einen Webbrowser einen extrem sicheren, softwareunabhängigen Mehrbenutzerzugriff auf die KVM-Konsolen Ihrer Server unter effizienter Ausnutzung der Bandbreite.

IP-Reach lässt sich mit dem Tastatur-, Video- und Mausport für bis zu vier Servern oder KVM-Switches verbinden. Mit der leistungsfähigen Frame-Grapper- und Videokomprimierungstechnologie von Raritan erfasst, digitalisiert und komprimiert IP-Reach das Videosignal vor der Übertragung an einen Remote-PC. Der Remotebenutzer verfügt über direkten Zugriff auf die Zielserver und kann diese zur Wartung, Verwaltung und Problembehandlung vollständig steuern. Er kann Anwendungen mit grafischer Benutzeroberfläche ausführen, eine Problembehandlung auf BIOS-Ebene durchführen und sogar Neustarts initiieren.

Mit IP-Reach lässt sich jederzeit und von überall bequem auf die Server zugreifen. Sie können:

- Server innerhalb des Firmengebäudes oder über das Firmengelände hinweg steuern
- Server in Zweigniederlassungen von einem zentralen Ort aus verwalten
- Remoteunterstützung für Rechenzentren weltweit bieten
- Problembehandlung, Rekonfiguration und Neustart von Servern von zu Hause aus vornehmen
- Bequeme und sichere entfernte Serververwaltung bieten

Zugriff über Internet, LAN/WAN oder DFÜ-Modem

IP-Reach bietet eine breite Palette an Remotezugriffsmethoden zur Steuerung von Servern, die mit einem KVM-Switch von Raritan verbunden sind. Da mit IP-Reach auch ein Out-of-Band-Zugriff der Server möglich ist, ist der Remotezugriff auf unternehmenskritische Zielserver jederzeit verfügbar, sogar bei einem Netzwerkausfall.

Produktfotos

IP-Reach M-Serie

IP-Reach TR-Serie

Paketinhalt

IP-Reach wird als vollständig konfiguriertes und eigenständiges Produkt in einem standardmäßigen 2U-19"-Gestellchassis geliefert. Ferner ist im Lieferumfang Folgendes enthalten:

TR-Serie

(1) IP-Reach-Einheit
(1) Kurzanleitung für die Installation und Konfiguration der IP-Reach-TR-Serie
(1) IP-Reach-Benutzerhandbuch
(1) Raritan Remote Client-Software CD-ROM
(1) Gestellmontagekit
(1) Netzkabel
(1) RJ11-Telefonkabel
(N) CCP20-Koaxialkabel
(N) CCP20F-Koaxialkabel

M-Serie

(1) IP-Reach-Einheit
(1) Kurzanleitung für die Installation und Konfiguration der IP-Reach-M-Serie
(1) IP-Reach-Benutzerhandbuch
(1) Raritan Remote Client-Software CD-ROM
(1) Gestellmontagekit
(1) Netzkabel
(N) CCP20-Koaxialkabel

(N = Anzahl der Ports)

Produktfeatures

Zugriff

- Remote-KVM-Zugriff über Internet, LAN/WAN oder DFÜ-Modem
- Bis zu vier Benutzerverbindungen zu(m) Switch(es) oder Server(n) gleichzeitig
- Bis zu 16 Benutzer gleichzeitig (im PC-Share-Modus)
- Webbrowser zugänglich
- Remotezugriff auf mit dem seriellen Port von IP-Reach verbundene serielle Geräte (VT100)

Leistung

- Überdurchschnittliche Komprimierungstechnologie für eine außergewöhnliche Leistung
- Keine Beeinträchtigung der Leistung der Zielserver
- Automatische Erkennung der Videoauflösung für eine optimale Anzeige
- Hochleistungs-Maustracking und -synchronisierung

Zuverlässigkeit

- Redundante ausfallsichere Netzteile*
- Redundantes ausfallsicheres Ethernet*
- Integriertes Modem*/Dedizierter Modemport** ermöglicht die Zugänglichkeit der Server auch bei Nichtverfügbarkeit des Netzwerks

Sicherheit

- Öffentlicher SSL-128-Bit-RSA-Schlüssel, 128-Bit-RC4-Privatschlüssel-Verschlüsselung
- Einzelner konfigurierbarer TCP-Port für den Firewallschutz
- Unterstützung von RADIUS- und LDAP-Authentifizierungsprotokollen

Administration

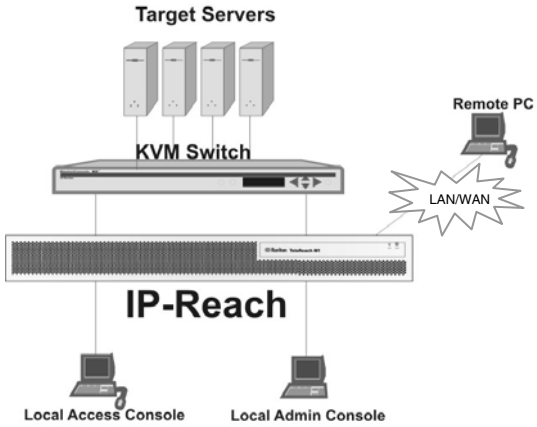
- Remoteadministration über die Webbrowserschnittstelle
- Enge Integration mit der Verwaltungsanwendung CommandCenter
- SNMP-Unterstützung
- Firmware über Ethernet aktualisierbar
- Vereinfachte Installations- und Benutzeroberfläche
- Benutzerkonsole für direkten analogen Zugriff auf KVM-Switch
- Umfangreiches herunterladbares Benutzerereignisprotokoll
- DHCP oder feste IP-Adressen

* nur IP-Reach TR-Serie

** nur IP-Reach M-Serie

Terminologie

In diesem Handbuch werden folgende Begriffe zur Bezeichnung der Komponenten einer typischen IP-Reach-Konfiguration verwendet. Ziehen Sie beim Lesen des Handbuchs bei Bedarf die nachstehende Tabelle zu Rate.



Zielserver	Server, auf die remote über IP-Reach und die damit verbundene KVM-Konfiguration zugegriffen werden soll.
Remote-PC	Ein Windows-Computer, mit dem der Zugriff und die Steuerung der mit IP-Reach verbundenen Zielserver erfolgt
Lokale Zugriffskonsole	Eine **optionale** Benutzerkonsole, bestehend aus einer PS/2-Tastatur, einer PS/2-Maus und einem VGA-Monitor, die direkt mit IP-Reach verbunden ist und die Zielserver lokal (nicht über das Netzwerk) steuern soll. Einzelport-IP-Reach-Modelle (IPR-TR361 und IPR-M1) lassen die Verbindung einer lokalen Zugriffskonsole zu. Dualport-IP-Reach-Modelle (IPR-TR362 und IPR-M2) ermöglichen die Verbindung von zwei lokalen Zugriffskonsolen, während Dreiport-IP-Reach-Modelle eine Verbindung zu drei Konsolen zulassen usw.
Lokale Verwaltungskonsole	Eine direkt mit IP-Reach verbundene PS/2-Tastatur und ein VGA-Monitor, die der Verwaltung und der Konfiguration dienen. Von dieser Konsole aus haben Sie direkten Zugriff auf die IP-Reach-Verwaltungsmenüs. Mit diesem Bildschirm können Sie keine Zielserver der verbundenen KVM-Konfiguration anzeigen. Obwohl IP-Reach auch eine Remoteverwaltung über das Netzwerk zulässt, bietet die lokale Verwaltungskonsole die bequemste Möglichkeit zur Durchführung der Erstkonfiguration.

Modellreihen

Raritan bietet zwei verschiedene IP-Reach-Modellreihen: die TR-Serie und die M-Serie. Beide Modellreihen verfügen über dieselben Features und die gleiche hohe Leistung. Die TR-Serie bietet allerdings folgende Hardwarevorteile, die von Anwendungen der Carrier-Klasse gefordert werden:

- Zwei redundante Netzteile
- Zwei ausfallsichere Ethernet-Controller
- Aktualisierbare Portdichte (bis zu vier Ports)
- Integriertes Modem
- 2U-Gestellhöhe

Kapitel 2: Installation

Konfigurieren der Zielserver

Vor dem Installieren von IP-Reach müssen Sie zur Gewährleistung einer optimalen Leistung zunächst die Zielserver konfigurieren, auf die Sie über IP-Reach zugreifen möchten (siehe unten). Die folgenden Konfigurationsanforderungen beziehen sich nur auf *Zielserver*, nicht auf die Computer, die Sie für den Remotezugriff auf IP-Reach verwenden (siehe **Kapitel 1: Einleitung, *Terminologie***).

Videoauflösung des Servers

Zur Gewährleistung einer optimalen Bandbreiteneffizienz und Videoleistung sollte der Desktophintergrund von Zielservern mit grafischer Benutzeroberfläche wie Windows, X-Windows, Solaris und KDE auf eine einfache Grafik mit glatten Farben eingestellt werden. Hintergründe mit Fotos oder komplexen Farbverläufen sollen vermieden werden.

Stellen Sie sicher, dass die Videoauflösung und Aktualisierungsfrequenz des Servers von IP-Reach unterstützt wird und das Signal keinen Zeilensprung beinhaltet. IP-Reach unterstützt die folgenden Videoauflösungen:

Textmodi

640x480 bei 60Hz	1024x768 bei 60Hz
640x480 bei 72Hz	1024x768 bei 70Hz
640x480 bei 75Hz	1024x768 bei 75Hz
640x480 bei 85Hz	1024x768 bei 85Hz
800x600 bei 56Hz	1152x864 bei 60Hz
800x600 bei 60Hz	1152x864 bei 75Hz
800x600 bei 72Hz	1280x1024 bei 60Hz
800x600 bei 75Hz	
800x600 bei 85Hz	

Einstellungen für Windows XP

Deaktivieren Sie auf Zielservern mit Microsoft Windows XP die Option **Zeigerbeschleunigung verbessern**, und stellen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung ein. Diese Parameter finden Sie unter **Systemsteuerung → Maus → Mauszeiger**.

Hinweis: *Für Zielserver, die Windows NT, 2000 oder XP ausführen, können Sie einen Benutzernamen erstellen, der nur für Remoteverbindungen über IP-Reach verwendet wird. Auf diese Weise können Sie die langsamen Einstellungen für die Mausgeschwindigkeit/-beschleunigung auf die IP-Reach-Verbindung beschränken, da andere Benutzer möglicherweise schnellere Mausgeschwindigkeiten benötigen.*

Hinweis: *Die Anmeldemasken von Windows XP und 2000 werden auf die voreingestellten Mausparameter zurückgesetzt. Diese Einstellungen unterscheiden sich von den für eine optimale Leistung von IP-Reach empfohlenen Einstellungen. In diesen Masken ist die Maussynchronisierung daher nicht optimal. Wenn Sie sich mit dem Anpassen der Registrierung von Windows-Zielservern auskennen, können Sie in den Anmeldemasken eine bessere IP-Reach-Maussynchronisierung erzielen, indem Sie hierzu mit dem Registrierungs-Editor von Windows die folgenden Einstellungen ändern: Default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0.*

Einstellungen für Windows 2000/ME

Stellen Sie auf Zielservern mit Microsoft Windows 2000/ME die Mausbeschleunigung auf **Keine** ein, und setzen Sie die Mausgeschwindigkeit genau auf die mittlere Geschwindigkeitseinstellung. Diese Parameter finden Sie unter **Systemsteuerung → Maus**.

Einstellungen für Windows 95/98/NT

Stellen Sie auf Zielservern mit Microsoft Windows 95/98/NT unter **Systemsteuerung → Maus → Bewegung** die Mausgeschwindigkeit auf die niedrigste Einstellung ein.

Einstellungen für Linux

Stellen Sie auf Zielservern mit grafischen Linux-Benutzeroberflächen die Mausbeschleunigung und den Schwellwert genau auf 1 ein.

Stellen Sie, wie oben erwähnt, sicher, dass jeder Linux-Zielserver eine von IP-Reach unterstützte Auflösung mit einer standardmäßigen VESA-Auflösung und Aktualisierungsfrequenz verwendet. Jeder Linux-Zielserver sollte zudem so eingestellt werden, dass die Deaktivierungszeiten bei +/- 40 % der VESA-Standardwerte liegen.

So überprüfen Sie diese Parameter:

- Wechseln Sie zur Xfree86-Konfigurationsdatei XF86Config.
- Deaktivieren Sie in einem Text-Editor alle nicht von IP-Reach unterstützten Auflösungen.
- Deaktivieren Sie das virtuelle Desktopfeature. Dieses Feature wird nicht von IP-Reach unterstützt.
- Ändern Sie die Deaktivierungszeiten (+/- 40 % des VESA-Standards).
- Starten Sie den Computer neu.

Hinweis: *In vielen grafischen Linux-Umgebungen ändert der Befehl <Strg+Alt+Plus> die Videoauflösung, indem ein Bildlauf durch alle verfügbaren (noch aktivierten) Auflösungen in der Datei XF86Config durchgeführt wird.*

Einstellungen für Sun Solaris

Für alle Zielserver muss eine von IP-Reach unterstützte Anzeigeauflösung konfiguriert werden. Die am häufigsten verwendeten unterstützten Auflösungen für Sun-Computer sind:

- 1024 x 768 bei 60 Hz
- 1024 x 768 bei 70Hz
- 1024 x 768 bei 75 Hz
- 1024 x 768 bei 85 Hz
- 1152 x 900 bei 66 Hz
- 1152 x 900 bei 76 Hz
- 1280 x 1024 bei 60 Hz

Zielserver mit dem Betriebssystem Solaris müssen VGA-Video ausgeben (H-und-V-Synchronisierung, keine zusammengesetzte Synchronisierung). Zum Ändern der Sun-Videokartenausgabe von der zusammengesetzten Synchronisierung zur nicht-standardmäßigen VGA-Ausgabe führen Sie zunächst den Befehl **Stop+A** aus, um den bootprom-Modus zu deaktivieren. Anschließend führen Sie den folgenden Befehl aus:

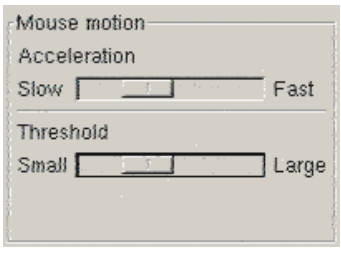
```
setenv output-device screen:r1024x768x70
```

Dadurch wird die Ausgabeauflösung geändert. Starten Sie den Server mit dem Befehl „boot“ neu.

Sie können sich stattdessen auch an Ihren Raritan-Ansprechpartner wenden und einen Videoausgabeadapter erwerben. 13W3 Sun-Systeme mit Composite-Synchronisierungsausgabe erfordern für die Verwendung mit IP-Reach einen APSSUN II Raritan Guardian-Converter. HD15 Sun-Systeme mit Composite-Synchronisierungsausgabe erfordern den 1396C Raritan-Converter für die Konvertierung von HD15 zu 13W3 und einen APSSUN II Raritan Guardian-Converter zur Unterstützung der Composite-Synchronisierung. HD15 SunSysteme mit separater Composite-Synchronisierungsausgabe erfordern für die Verwendung mit IP-Reach einen APKMSUN Raritan Guardian-Converter.

Bei KVM-Switchmarken, die nicht mit den Marken von Raritan übereinstimmen, ist die ordnungsgemäße Verarbeitung von PS/2-zu-Sun-Signalen nicht unbedingt gewährleistet.

Stellen Sie auf Zielservern mit dem Betriebssystem Solaris die Mausbeschleunigung und den Schwellwert genau auf 1 ein. Diese Einstellung kann über die grafische Benutzeroberfläche (siehe unten) oder die Befehlszeile „xset mouse a t“ vorgenommen werden, wobei „a“ für die Beschleunigung und „t“ für den Schwellwert steht.



Einstellungen für Apple Macintosh

Für Zielserver mit einem Apple Macintosh-Betriebssystem muss der IP-Reach-Client (Raritan Remote Client) auf den Modus „ein Cursor“ eingestellt werden, wenn Sie IP-Reach für den Zugriff und die Steuerung des Zielservers verwenden. Der Modus mit zwei Cursorn wird nicht unterstützt. Die zwei Mauszeiger werden nicht synchronisiert angezeigt, wenn Sie versuchen, einen Macintosh-Server in diesem Modus über IP-Reach zu steuern.

Konfigurieren der Einstellungen für die Netzwerkfirewall

Wenn Sie über eine Netzwerkfirewall auf IP-Reach zugreifen möchten, muss die Firewall die Kommunikation über TCP-Port 5000 zulassen. IP-Reach kann auch zur Verwendung eines anderen TCP-Ports Ihrer Wahl konfiguriert werden (siehe **Kapitel 4: Verwaltungsfunktionen,** ***Netzwerkkonfiguration***).

Wenn Sie die Webzugriffsfunktionen von IP-Reach nutzen möchten, muss die Firewall auch die eingehende Kommunikation über TCP-Port 443 (den Standard-TCP-Port für HTTPS-Kommunikation) zulassen. Wenn Sie die Funktion von IP-Reach zur automatischen Umleitung von HTTP-Anforderungen an HTTPS nutzen möchten (damit Benutzer „http://xxx.xx.xxxx“ statt „https://xxx.xx.xxxx“ eingeben können), muss die Firewall auch die eingehende Kommunikation über TCP-Port 80 (den Standard-TCP-Port für HTTP-Kommunikation) zulassen.

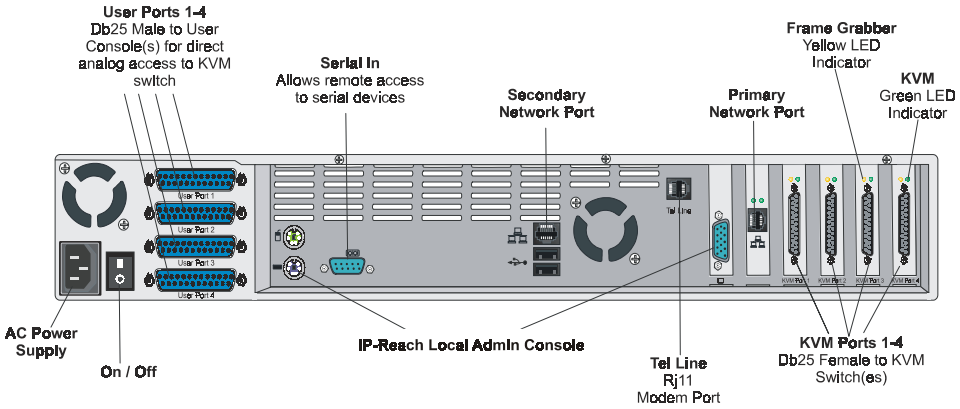
Konfigurieren von Paragon-KVM-Switches

Wenn Sie mit IP-Reach auf den Raritan Paragon-KVM-Switch der Unternehmensklasse zugreifen, führen Sie vor dem Anschließen von IP-Reach folgende Optimierungsschritte durch.

Zeigen Sie jeden Zielserver, der von der Paragon-Benutzerstation aus zugänglich ist, nacheinander an und stellen Sie die Videoverstärkungseinstellung auf -15 (minus 15) ein. Passen Sie die Paragon-Videoverstärkung bei gleichzeitiger Anzeige der Bildschirmbenutzerschnittstelle über die Plus- und Minustaste auf dem Ziffernblock an.

Während der Anzeige wird in der unteren Zeile des Bildschirmbenutzerschnittstellenmenüs angezeigt, wie sich die Verstärkungsparameter beim Drücken der Plus- und Minustaste verändern. Verstärkungseinstellungen von minus 15 ergeben die schärfste Bildeinstellung, wenn jeder Zielserver über IP-Reach von einem Remote-PC angezeigt wird. Nehmen Sie diese Einstellung für jeden Zielserver und jede Benutzerstation vor, die mit IP-Reach verbunden wird.

Physische Anschlüsse der TR-Serie



Rückseite des Modells IP-Reach TR-Serie

Netzkabel

Verbinden Sie das beiliegende Netzkabel mit IP-Reach, und schließen Sie es an die Wechselstromversorgung an.

Lokale Verwaltungskonsole

Schließen Sie eine PS/2-Tastatur und einen Multi-Sync-Monitor an die entsprechenden Ports (siehe Abbildung oben) auf der Rückseite von IP-Reach an.

Primärer Netzwerkport

Verbinden Sie den Netzwerkport über ein standardmäßiges Ethernet-Kabel mit einem Ethernet-Switch, -Hub oder -Router.

Sekundärer Netzwerkport (optional)

Verbinden Sie den Netzwerkport über ein standardmäßiges Ethernet-Kabel mit einem Ethernet-Switch, -Hub oder -Router. IP-Reach wechselt automatisch auf den sekundären Netzwerkport, wenn der primäre Netzwerkport nicht verfügbar ist. Weitere Anweisungen zum Aktivieren der ausfallsicheren Ethernet-Unterstützung finden Sie in **Kapitel 4: Verwaltungsfunktionen, *Netzwerkkonfiguration***.

KVM-Eingangsports

Verbinden Sie den Port „KVM In“ über das mitgelieferte CCP20-Kabel mit der KVM-Konsole des Servers oder mit dem KVM-Switch, auf den remote zugegriffen werden soll.

KVM-Ausgangsports/Ports der lokalen Zugriffskonsole (optional)

Benutzerports „KVM Out“ ermöglichen einen direkten analogen Zugriff auf den Server oder den KVM-Switch, der mit den entsprechenden KVM-Eingangsports verbunden ist. Schließen Sie eine PS/2-Tastatur, PS/2-Maus und einen MultiSync-VGA-Monitor über das mitgelieferte CCP20F-Kabel an die Ports mit der Bezeichnung „User Port“ an.

Hinweis: *Lokale Zugriffskonsolen können an die Benutzerports 1 bis 4 angeschlossen werden. Jede lokale Zugriffskonsole zeigt den KVM-Switch oder den Server an, der mit dem entsprechenden KVM-Port verbunden ist. Die mit dem Benutzerport 1 verbundene Benutzerkonsole zeigt beispielsweise den KVM-Switch oder den*

Server an, der mit KVM-Port 1 verbunden ist. Die mit Benutzerport 2 verbundene Benutzerkonsole zeigt den KVM-Switch oder den Server an, der mit KVM-Port 2 verbunden ist usw.

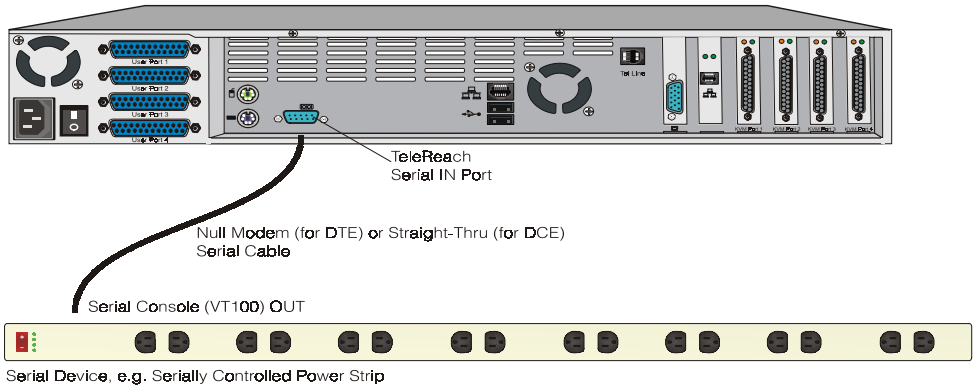
Telefonleitungsport (optional)

Die TR-Serie von IP-Reach ist mit einem integrierten Modem für den Remotezugriff ausgestattet, wenn das LAN/WAN nicht verfügbar ist. Verbinden Sie den Port mit der Bezeichnung „Tel Line“ über das mitgelieferte Telefonkabel mit einer analogen Telefonbuchse.

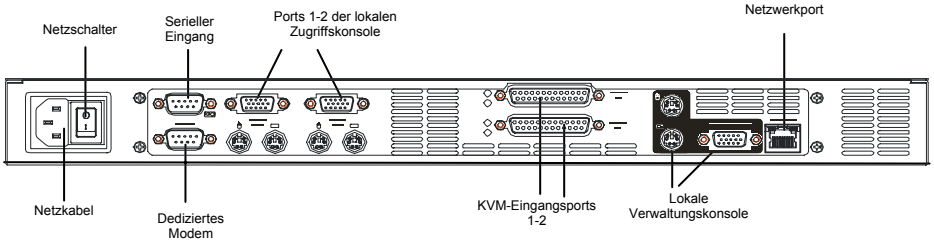
Serieller Eingangsport (optional)

Auf seriell gesteuerte Geräte (VT100-Terminalemulation) kann über IP-Reach remote zugegriffen werden, wenn sie mit dem seriellen Eingangsport („IN“) auf der Rückseite von IP-Reach verbunden werden.

Der serielle Port von IP-Reach entspricht dem Typ DTE. Verwenden Sie zum Anschließen eines anderen seriellen DTE-Geräts an IP-Reach ein serielles Null-Modem-Kabel. Zum Anschließen eines seriellen DCE-Geräts an IP-Reach verwenden Sie ein serielles Durchsteckkabel.


TeleReach
Serial IN Port
Null Modem (for DTE) or Straight-Thru (for DCE)
Serial Cable
Serial Console (VT100) OUT
Serial Device, e.g. Serially Controlled Power Strip

Physische Anschlüsse der M-Serie



Rückseite des Modells IP-Reach M-Serie

Netzkabel

Verbinden Sie das beiliegende Netzkabel mit IP-Reach, und schließen Sie es an die Wechselstromversorgung an.

Lokale Verwaltungskonsole

Schließen Sie eine PS/2-Tastatur und einen MultiSync-Monitor an die entsprechenden Ports mit der Bezeichnung „Admin Console“ (Verwaltungskonsole) auf der Rückseite des IP-Reach-Geräts an.

Netzwerkport

Verbinden Sie den Netzwerkport über ein standardmäßiges Ethernet-Kabel mit einem Ethernet-Switch, -Hub oder -Router.

KVM-Eingangsports

Verbinden Sie das DB25-Ende eines beiliegenden CCP20-Kabels mit den „KVM"-Ports und das andere Ende des CCP-Kabels mit den entsprechenden PS/2-Tastatur-, Maus- und VGA-Videoports der KVM-Switches oder Server, für die der Remotenetzwerkzugriff eingerichtet werden soll.

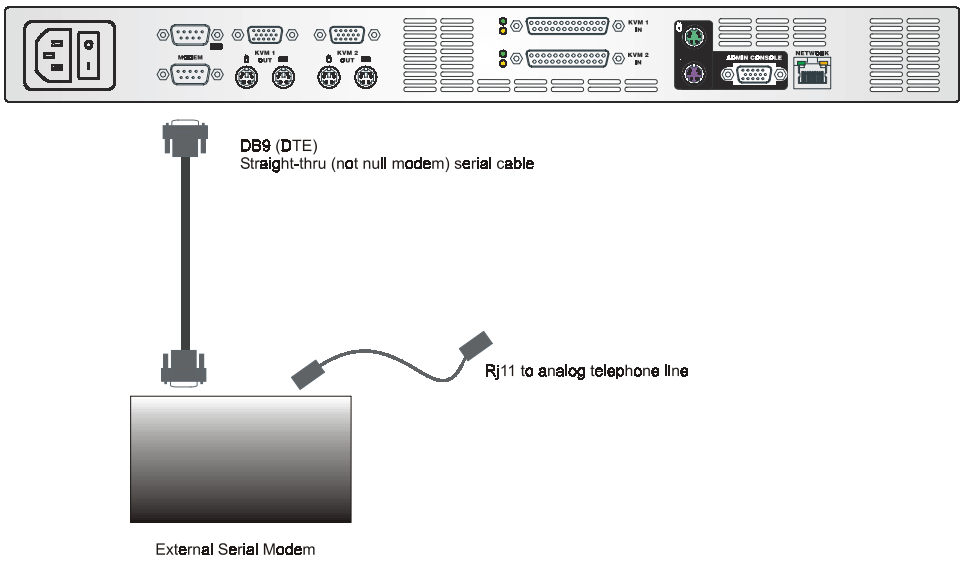
KVM-Ausgangsports/Ports der lokalen Zugriffskonsole (optional)

Schließen Sie eine PS/2-Tastatur, Maus und einen MultiSync-Monitor an diese Ports an, wenn Sie lokalen direkten analogen Zugriff auf die Server oder KVM-Switches einrichten möchten, die mit den entsprechenden Ports „KVM In" verbunden sind.

Hinweis: *Beim Modell M2 von IP-Reach zeigt die mit einem KVM-Ausgangsport verbundene lokale Zugriffskonsole den KVM-Switch oder Server an, der an die entsprechende KVM-Eingangsportnummer angeschlossen ist. Die an den KVM-Ausgangsport 1 angeschlossene Benutzerkonsole zeigt den KVM-Switch oder Server an, der mit dem KVM-Eingangsport 1 verbunden ist.*

Dedizierter Modemport (optional)

Die IP-Reach-Modelle der M-Serie sind mit einem dedizierten Modemport ausgestattet. Durch Anschließen eines standardmäßigen externen seriellen Modems an diesen Port kann unter Umständen der Remotezugriff auf IP-Reach bestehen bleiben, wenn das LAN/WAN nicht verfügbar ist.



Verwenden Sie zum Verbinden von IP-Reach mit dem externen seriellen Modem ein standardmäßiges serielles Durchsteckkabel. Verbinden Sie anschließend den Port „Tel Line" des Modems mit einer analogen Telefonleitung (nähere Informationen dazu finden Sie in der Dokumentation Ihres externen seriellen Modems).

Serieller Eingangsport (optional)

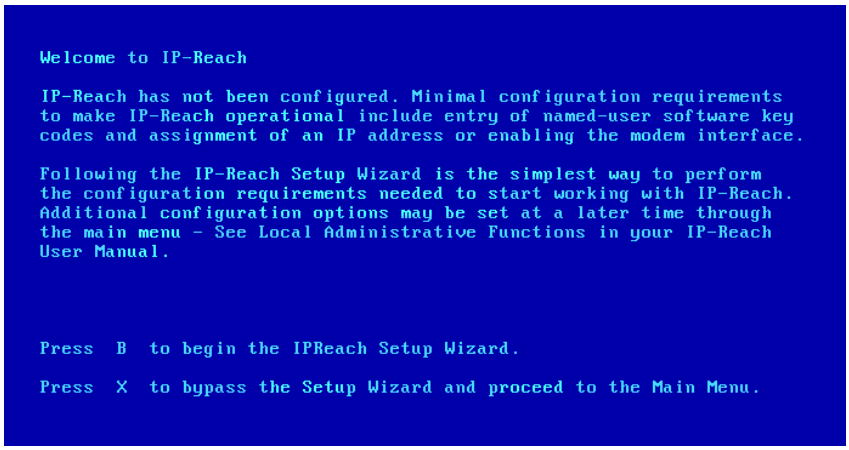
Auf seriell gesteuerte Geräte (VT100-Terminalemulation) kann über IP-Reach remote zugegriffen werden, wenn sie mit dem seriellen Eingangsport („IN") auf der Rückseite von IP-Reach verbunden werden.

Der serielle Port von IP-Reach entspricht dem Typ DTE. Verwenden Sie zum Anschließen eines anderen seriellen DTE-Geräts an IP-Reach ein serielles Null-Modem-Kabel. Zum Anschließen eines seriellen DCE-Geräts an IP-Reach verwenden Sie ein serielles Durchsteckkabel.

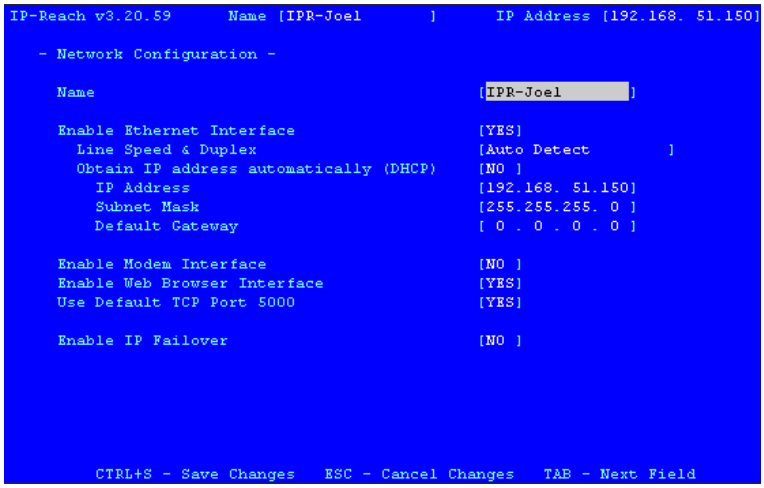
Erstkonfiguration

Der **IP-Reach Setup Wizard** (Konfigurationsassistent von IP-Reach) hilft Ihnen, die Einstellungen für die Erstkonfigurationen vorzunehmen. Der IP-Reach Setup Wizard erscheint nur, wenn auf einem nicht konfigurierten IP-Reach-Gerät auf die Administrationsmenüs zugegriffen wird. Er führt Sie durch die Einstellungsschritte der Parameter für die Erstkonfiguration. Die einfachste Möglichkeit, die Erstkonfiguration vorzunehmen, besteht darin, die lokale Verwaltungskonsole zu verwenden (siehe die Anweisungen unter „Physische Anschlüsse“ in einem der vorherigen Abschnitte).

1. Schalten Sie das IP-Reach-Gerät mit dem Netzschalter auf der Rückseite des Geräts auf „ON“ (EIN).
2. Der Begrüßungsbildschirm des IP-Reach Setup Wizard wird in der lokalen Verwaltungskonsole angezeigt.


Welcome to IP-Reach
IP-Reach has not been configured. Minimal configuration requirements to make IP-Reach operational include entry of named-user software key codes and assignment of an IP address or enabling the modem interface.
Following the IP-Reach Setup Wizard is the simplest way to perform the configuration requirements needed to start working with IP-Reach. Additional configuration options may be set at a later time through the main menu - See Local Administrative Functions in your IP-Reach User Manual.
Press B to begin the IPReach Setup Wizard.
Press X to bypass the Setup Wizard and proceed to the Main Menu.

3. Drücken Sie den Buchstaben <**B**> auf der Tastatur der lokalen Verwaltungskonsole, um den IP-Reach Setup Wizard zu starten.
4. Der Bildschirm **Network Configuration** (Netzwerkkonfiguration) wird angezeigt.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Network Configuration -
Name [IPR-Joel]
Enable Ethernet Interface [YES]
Line Speed & Duplex [Auto Detect]
Obtain IP address automatically (DHCP) [NO]
IP Address [192.168. 51.150]
Subnet Mask [255.255.255. 0]
Default Gateway [0 . 0 . 0 . 0]
Enable Modem Interface [NO]
Enable Web Browser Interface [YES]
Use Default TCP Port 5000 [YES]
Enable IP Failover [NO]
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

5. Wählen Sie die einzelnen Zeilen im Fenster **Network Configuration** (Netzwerkkonfiguration) mit den Tasten <**Tab**>, <↑> oder <↓> aus, und wechseln Sie mit der LEERTASTE oder der Taste <←> oder <→> zwischen den verfügbaren Einträgen hin und her. Drücken Sie die EINGABETASTE, die <**Tab**>-Taste oder die Taste <↓>, sobald die Einträge in jeder Zeile abgeschlossen sind. Nachstehend sind Beschreibungen jedes einzelnen Felds sowie die entsprechenden zuzuweisenden Werte aufgeführt.

- **Name:** Vergeben Sie einen eindeutigen Namen für diese IP-Reach-Einheit, zum Beispiel „Hamburger Rechenzentrum“. Der Standardname lautet **IP-Reach**.
- **Enable Ethernet Interface** (Ethernet-Schnittstelle aktivieren)**:** Gibt an, ob IP-Reach seinen Ethernet-Adapter als aktiv zulassen soll (Standardeinstellung: YES).

Hinweis: *Bei den Netzwerkverbindungen muss es sich um 10BASE-T oder 100BASE-TX Ethernet handeln.*

- **Line Speed & Duplex** (Übertragungsrate und Duplex)**:** Geben Sie das visuelle Leistungsmerkmal für den Monitor ein: Auto detect 10 Mbps/Full Duplex (Automatische Erkennung 10 MBit/s/Vollduplex), 10 Mbps/Half Duplex (10 MBit/s/Halbduplex), 100 Mbps/Full Duplex (100 MBit/s/Vollduplex) oder 100 Mbps/Half Duplex (100 MBit/s/Halbduplex).

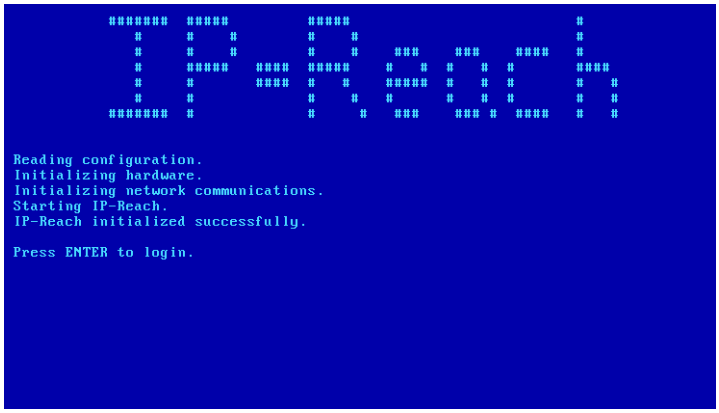
- **Obtain IP address automatically (DHCP)** (IP-Adresse automatisch zuweisen [DHCP])**:**
  - ♦ **YES** (JA)**:** Aktiviert dynamische IP-Adressen für IP-Reach. Bei jedem Starten von IP-Reach wird eine IP-Adresse vom lokalen DHCP-Server angefordert. Diese Einstellung kann den Remotezugriff auf IP-Reach von außerhalb des LANs erschweren, da die dynamisch zugewiesene IP-Adresse bekannt sein muss, um eine Verbindung zu initiieren.
  - ♦ **NO** (NEIN)**, Standardeinstellung:** Weist der IP-Reach-Einheit eine feste IP-Adresse zu (empfohlen).
    - ▪ **IP Address** (IP-Adresse)**:** Geben Sie die von Ihrem Netzwerkadministrator vergebene IP-Adresse für IP-Reach ein.
    - ▪ **Subnet Mask** (Subnetzmaske)**:** Geben Sie eine Subnetzmaske ein. Diese erhalten Sie von Ihrem Netzwerkadministrator.
    - ▪ **Default Gateway** (Standardgateway)**:** Geben Sie das Standardgateway ein, sofern Ihr Netzwerkadministrator ein Gateway benennt.

- **Enable Modem Interface** (Modemschnittstelle aktivieren)**:** Aktiviert den Zugriff auf das DFÜ-Modem (Standard: YES). Bei IP-Reach-Modellen der M-Serie muss ein externes serielles Modem angeschlossen sein, damit diese Funktion ordnungsgemäß funktioniert (siehe **Kapitel 2: Installation,** ***Physische Anschlüsse der M-Serie, Dedizierter Modemport***).
- **Enable Web Browser Interface** (Webbrowserschnittstelle aktivieren)**:** Aktiviert den Webbrowserzugriff auf IP-Reach (Standard: YES).
- **Use Default TCP Port 5000** (Standard-TCP-Port 5000 verwenden)**:**
  - **YES** (JA)**, Standardeinstellung:** Verwendet den Standardport 5000.
  - **NO** (NEIN)**:** Geben Sie eine alternative Portnummer ein.

Hinweis: *Wenn Sie über eine Firewall auf IP-Reach zugreifen möchten, müssen die Firewalleinstellungen die ein- und ausgehende Kommunikation über den Standardport 5000 bzw. den nicht standardmäßigen konfigurierten Port zulassen.*

- **Enable IP Failover** (IP-Ausfallsicherung aktivieren) (nur TR-Serie)**:** Diese Einstellung, die nur für Modelle der TR-Serie angezeigt wird, aktiviert den sekundären Ethernet-Port für die Ausfallsicherung.
  - Ist sie aktiviert, prüft IP-Reach die Verfügbarkeit des primären Ethernet-Ports in regelmäßigen Abständen. Der Intervall wird in der Einstellung **Ping Interval in seconds** (Pingintervall in Sekunden) festgelegt.
  - Wenn der primäre Ethernet-Port bei jeder regelmäßigen Pingüberprüfung für einen längeren Intervall nicht verfügbar ist, als in der Einstellung **Failover Timeout in seconds** (Ausfallsicherungszeitlimit in Sekunden) angegeben, deaktiviert IP-Reach seinen primären Ethernet-Port automatisch und aktiviert den sekundären Ethernet-Port.
  -

6. Drücken Sie zum Speichern der Einträge <**Strg+S**>. Das Hauptmenü wird angezeigt.
7. Wählen Sie im Hauptmenü **[R] Restart or shutdown the IP-Reach** (IP-Reach neu starten oder herunterfahren) und drücken Sie die EINGABETASTE.
8. Drücken Sie auf den Buchstaben <**R**> auf der Tastatur, wenn Sie dazu aufgefordert werden, um IP-Reach neu zu starten.
9. IP-Reach wird neu gestartet und das IP-Reach Fenster **Initialization** (Initialisierung) angezeigt.



10. Gratulation! IP-Reach ist nun bereit für die erste Verbindung.

Fahren Sie mit dem nächsten Abschnitt fort, um die erste Remoteverbindung zu IP-Reach zu initiieren. Sobald Sie sich mit dem Remotebetrieb von IP-Reach vertraut gemacht haben, lesen Sie **Kapitel 4: Verwaltungsfunktionen**. Hier werden die vollständigen Verwaltungsfunktionen, die IP-Reach bietet, vorgestellt.

Herstellen einer Remoteverbindung zu IP-Reach

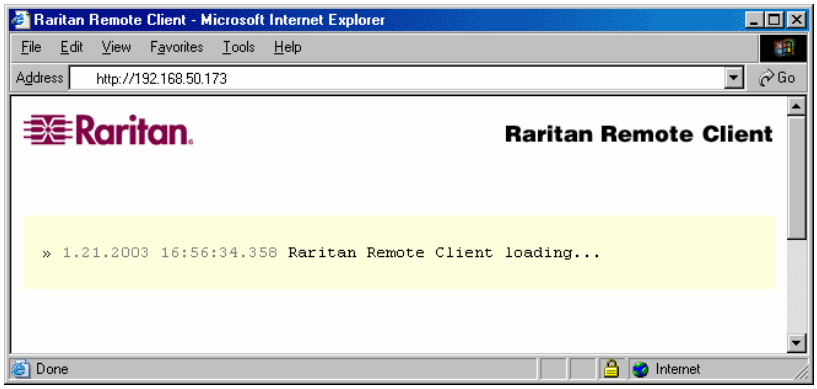
Nach abgeschlossener physischer Installation von IP-Reach kann nun die erste Netzwerkverbindung hergestellt werden. Führen Sie dazu die nachstehenden Anweisungen aus. Ausführlichere Anweisungen erhalten Sie in **Kapitel 3: Raritan Remote Client**.

Starten von Raritan Remote Client (RRC)

1. Melden Sie sich an einem Windows-Computer an, der Netzwerkzugriff auf IP-Reach besitzt.
2. Bei Verwendung von Windows NT, 2000 oder XP müssen Sie sicherstellen, dass Sie über die entsprechenden Berechtigungen verfügen.
3. Starten Sie Microsoft Internet Explorer. Stellen Sie sicher, dass die Internet Explorer-Sicherheitseinstellungen den Download und die Ausführung von ActiveX-Steuerelementen zulassen.

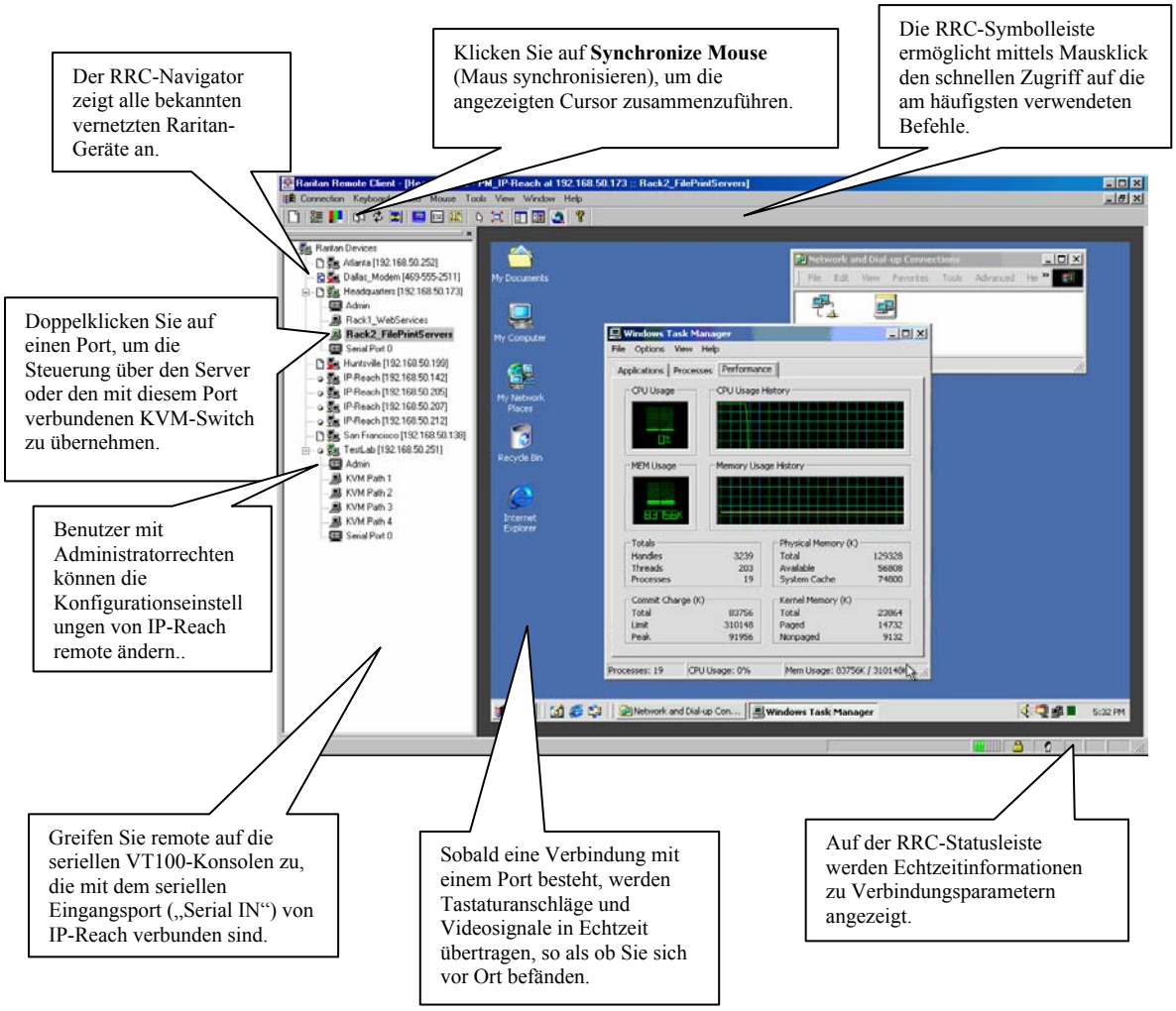
Hinweis: *Die standardmäßige Windows-Sicherheitseinstellung* ***Mittel*** *ist ausreichend.*

4. Geben Sie in das URL-Adressfeld die IP-Adresse ein, die Sie IP-Reach in Schritt II-6 zugewiesen haben. Drücken Sie die EINGABETASTE, um den Webzugriffsclient zu laden und zu starten.



Einrichten einer Verbindung

Beim Starten von Raritan Remote Client (RRC) fordert IP-Reach Ihre Benutzerdaten an. Melden Sie sich mit dem standardmäßigen Benutzernamen und Kennwort (<admin> und <raritan>) an. Die Verbindung zur IP-Reach-Einheit wird hergestellt. Verwenden Sie den RRC-Navigator auf der linken Seite des RRC-Fensters, um einen Port auszuwählen und eine Verbindung mit diesem Port herzustellen.


Der RRC-Navigator zeigt alle bekannten vernetzten Raritan-Geräte an.
Klicken Sie auf **Synchronize Mouse** (Maus synchronisieren), um die angezeigten Cursor zusammenzuführen.
Die RRC-Symbolleiste ermöglicht mittels Mausklick den schnellen Zugriff auf die am häufigsten verwendeten Befehle.
Doppelklicken Sie auf einen Port, um die Steuerung über den Server oder den mit diesem Port verbundenen KVM-Switch zu übernehmen.
Benutzer mit Administratorrechten können die Konfigurationseinstell ungen von IP-Reach remote ändern..
Greifen Sie remote auf die seriellen VT100-Konsolen zu, die mit dem seriellen Eingangsport („Serial IN“) von IP-Reach verbunden sind.
Sobald eine Verbindung mit einem Port besteht, werden Tastaturanschläge und Videosignale in Echtzeit übertragen, so als ob Sie sich vor Ort befänden.
Auf der RRC-Statusleiste werden Echtzeitinformationen zu Verbindungsparametern angezeigt.

Hinweis für CommandCenter-Benutzer

Wenn Sie IP-Reach in einer CommandCenter-Konfiguration verwenden, führen Sie die Installationsschritte wie oben beschrieben aus. Nachdem Sie die in diesem Kapitel beschriebenen Schritte ausgeführt haben, ziehen Sie das CommandCenter-Benutzerhandbuch zu Rate, um die Installation fortzusetzen. Der Rest dieses Benutzerhandbuchs richtet sich in erster Linie an Benutzer, die ihre IP-Reach-Einheit(en) ohne die Integrationsfunktion von CommandCenter bereitstellen.

Kapitel 3: Raritan Remote Client

Aufrufen von Raritan Remote Client (RRC) über einen Webbrowser

IP-Reach verfügt über Webbrowser-Zugriffsfunktionen, die über einen beliebigen Windows-Remote-PC, auf dem Microsoft Internet Explorer 4.0+, Mozilla 1.1+ oder Netscape 7+ ausgeführt wird, eine Verbindung herstellen.

Sicherheitseinstellungen

Für den Zugriff auf IP-Reach über einen Webbrowser sind entsprechende Einstellungen auf der Registerkarte mit den Sicherheitseinstellungen von Internet Explorer erforderlich:

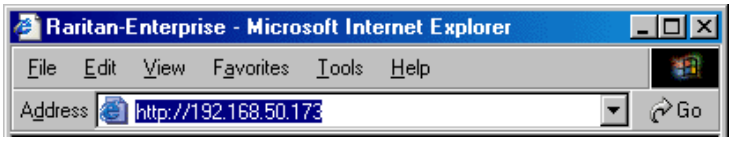
- **Download von signierten ActiveX-Steuerelementen** sollte auf **Aktivieren** oder **Fragen** gesetzt werden.
- **ActiveX-Steuerelemente und Plugins ausführen** sollte auf **Aktivieren** oder **Fragen** gesetzt werden.

Ausführliche Informationen zu diesen Einstellungen finden Sie in Ihrer Microsoft Internet Explorer-Dokumentation.

Hinweis: *Unter Microsoft Windows 2000 und Microsoft Windows XP können bestimmte Benutzertypen unabhängig von den obigen Einstellungen in Internet Explorer keine ActiveX-Steuerelemente und -Plugins downloaden und ausführen. Weitere Informationen finden Sie in Ihrer Microsoft Windows-Dokumentation.*

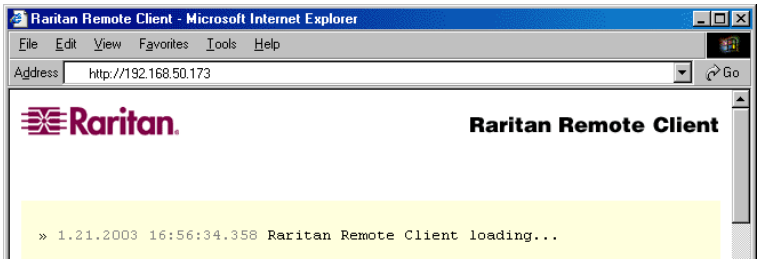
Starten von Raritan Remote Client

1. Geben Sie nach dem Bestätigen der ordnungsgemäßen Konfiguration Ihrer Browsersicherheitseinstellungen die IP-Adresse, die Ihrer IP-Reach-Einheit zugewiesen wurde (siehe **Kapitel 2: Installation, *Erstkonfiguration***), in das URL-Adressfeld Ihres Webbrowsers ein.



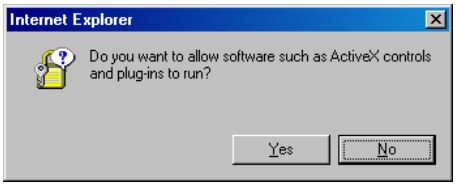
Hinweis: *IP-Reach wird mit der Standard-IP-Adresse 192.168.0.192 geliefert.*

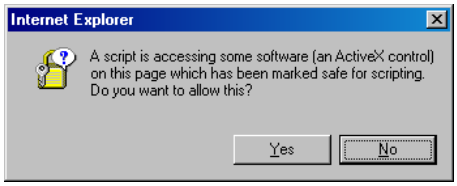
2. IP-Reach leitet Sie zum Starten von RRC zu einer sicheren HTTPS-Webseite (128 Bit) um.



3. Je nach Sicherheitskonfiguration Ihres Browsers werden ggf. die folgenden Dialogfelder zur Bestätigung des Zugriffs und Starts eines extern bereitgestellten Programms angezeigt. Klicken Sie in diesen Eingabeaufforderungen auf **Yes** (Ja).

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate




Internet Explorer
A script is accessing some software (an ActiveX control) on this page which has been marked safe for scripting. Do you want to allow this?
Yes
No

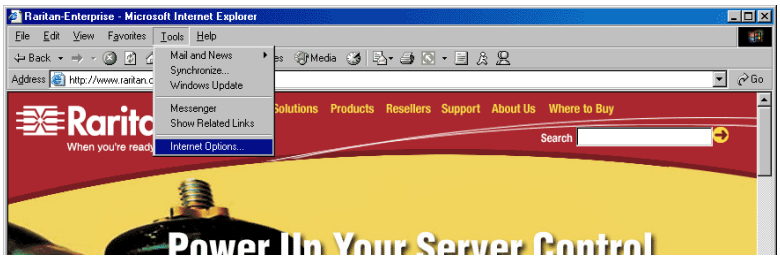
Hinweis: *Unter Microsoft Windows 2000 und Microsoft Windows XP können bestimmte Benutzertypen unabhängig von den obigen Einstellungen in Internet Explorer und unabhängig von Ihrer Bestätigung der oben angegebenen Warnungen keine ActiveX-Steuerelemente und -Plugins downloaden und ausführen. Weitere Informationen finden Sie im vorhergehenden Abschnitt „**Sicherheitseinstellungen**“ sowie in der Microsoft Windows-Dokumentation.*

Entfernen von RRC aus dem Browsercache

Verwenden Sie zum Entfernen von RRC aus Ihrem Browsercache, sei es, um eine Aktualisierung vorzunehmen, Festplattenspeicher einzusparen oder Beweise für das Ausführen von RRC auf einem PC zu beseitigen, das Ihrer Webbrowsersoftware entsprechende Standardverfahren.

Anweisungen für Internet Explorer 6.0:

1. Wenn Sie RRC kürzlich verwendet haben, beenden Sie Internet Explorer, und starten Sie das Programm neu.
2. Wählen Sie auf der Internet Explorer-Menüleiste die Befehle **Extras** → **Internetoptionen**.



3. Klicken Sie im Dialogfeld **Internetoptionen** auf **Einstellungen**.
4. Das Dialogfeld **Einstellungen** wird angezeigt. Klicken Sie auf **Objekte anzeigen**.
5. Internet Explorer zeigt eine Liste der zwischengespeicherten Programmobjekte an. Wählen Sie alle Einträge mit der Bezeichnung „TeleControl Class“ aus und löschen Sie sie.

Optional: Installieren von Raritan Remote Client-Software

Hinweis: *Dieser Schritt ist optional. Sie können von einem Remote-PC aus auf IP-Reach zugreifen, indem Sie entweder die RRC-Software installieren oder RRC über einen Webbrowser starten (siehe hierzu den vorhergehenden Abschnitt). Der Webbrowserzugriff auf IP-Reach erfordert keine Softwareinstallation auf dem Remote-PC.*

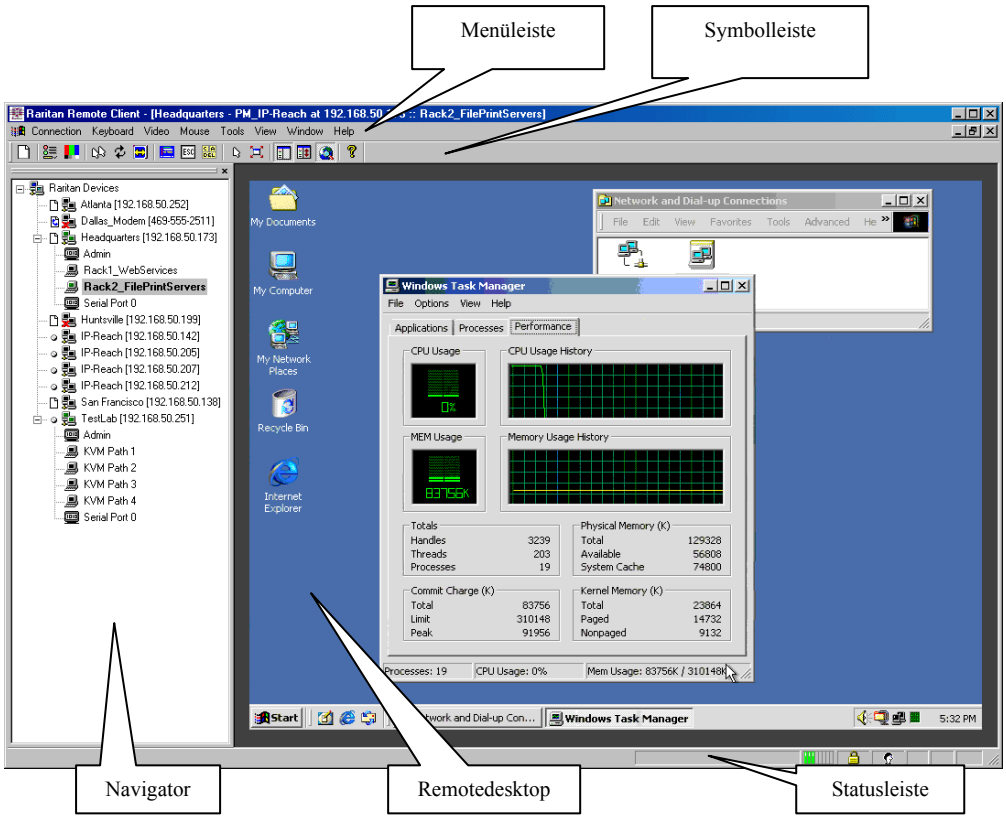
1. Legen Sie die mitgelieferte RRC-CD-ROM in das CD-ROM-Laufwerk Ihres PC ein.
2. Das RRC-Setupprogramm wird automatisch ausgeführt. Wenn dies nicht der Fall ist, klicken Sie im Windows Explorer mit der rechten Maustaste auf das CD-ROM-Laufwerk, und wählen Sie **Auto Play**.
3. Folgen Sie den Anweisungen des InstallShield-Assistenten, um die RRC-Installation auf dem Remote-PC fertig zu stellen. Wählen Sie unter **Select Components** (Komponenten auswählen) entweder die US-Version für eine US-amerikanische Remote-PC-Tastatur oder die japanische Version für eine japanische Remote-PC-Tastatur.

Hinweis: *Die japanische Version von RRC ermöglicht eine japanische Tastatur am Remote-PC und erfordert darüber hinaus eine japanische Tastatur am Zielserver. Die Benutzeroberflächeninformationen bleiben auf Englisch.*

4. Je nach Konfiguration des PC installiert das RRC-Installationsprogramm ggf. automatisch DirectX- und Microsoft Foundation Class-Bibliotheken. In diesem Fall werden Sie angewiesen, den PC nach der Installation neu zu starten.
5. Auf dem Desktop wird nun ein Raritan Remote Client-Symbol angezeigt. Klicken Sie auf dieses Symbol, um RRC zu starten.

RRC-Fensteranordnung

Die Raritan Remote Client-Funktionen werden in fünf allgemeinen Abschnitten auf dem Bildschirm angeordnet. Jeder dieser Bereiche wird in diesem Kapitel ausführlich behandelt.



RRC-Navigator

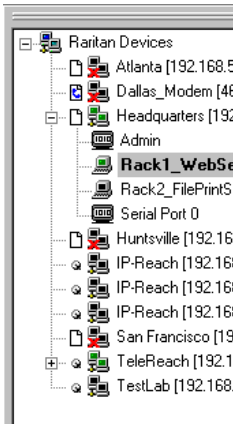
Der RRC-Navigator zeigt alle bekannten Raritan-Geräte in nur einer Ansicht an und bietet so bequemen Zugriff auf mehrere vernetzte Raritan-Geräte.

Der RRC-Navigator zeigt Folgendes an:

- Alle Raritan-Geräte, für die ein *Verbindungsprofil* vorhanden ist
- Alle Raritan-Geräte, die im Netzwerk automatisch identifiziert werden

Hinweis: *Die automatische Erkennung von Raritan-Geräten erfolgt mithilfe des UDP-Protokolls und identifiziert normalerweise alle Raritan-Geräte in Ihrem Subnetz. Netzwerkadministratoren lassen die Verwendung von UDP außerhalb eines Subnetzes selten zu.*

Hinweis: *Mit der automatischen Erkennung von Raritan-Geräten werden nur Raritan-Geräte gefunden, die für den Standard-TCP-Port (5000) konfiguriert sind.*



Jeder Geräteeintrag im RRC-Navigator enthält zwei Symbole zur Anzeige des Netzwerkstatus und der Verbindungsprofilinformationen.

Linkes Symbol (Verbindungsprofil)

	Profil erstellt – Für dieses Gerät ist ein Netzwerkverbindungsprofil vorhanden.
	Modemprofil – Für dieses Gerät ist ein Modemverbindungsprofil vorhanden.
	Kein Profil erstellt – RRC hat dieses Gerät im Netzwerk gefunden, es ist jedoch kein zugehöriges Verbindungsprofil vorhanden.

Rechtes Symbol (Netzwerkstatus)

	Verbunden (grün) – Sie sind zurzeit authentifiziert und mit diesem Gerät verbunden.
	Verfügbar (schwarz) – Dieses Gerät ist zurzeit im Netzwerk verfügbar, Sie sind jedoch nicht mit dem Gerät verbunden.
	Nicht verfügbar – Für dieses Gerät ist ein Profil vorhanden, es ist jedoch zurzeit nicht im Netzwerk verfügbar. (Dieses Symbol wird für alle Geräte mit Modemprofilen angezeigt, mit denen Sie zurzeit nicht verbunden sind.)

Für jedes verbundene Raritan-Gerät erweitert der RRC-Navigator die Strukturansicht, um die verfügbaren Ports anzuzeigen.

- Ein grünes Symbol zeigt an, dass Sie mit diesem Port verbunden sind.
- Der zurzeit im Remotedesktopbereich des Clients angezeigte Port (aktiv) ist fett hervorgehoben.

Navigator-Optionen

Bestimmte Attribute des RRC-Navigators können angepasst werden.

	Navigator ein-/ausblenden – Blendet den RRC-Navigator ein bzw. aus. Diese Option kann auch über die Befehlsfolge **View** → **Navigator** (Anzeige → Navigator) auf der Menüleiste umgeschaltet werden.
	Navigator aktualisieren – Aktualisiert die angezeigten Gerätestatusinformationen im RRC-Navigator.
	Gefundene Geräte anzeigen – Ermöglicht das Umschalten des RRC-Navigators, so dass entweder alle automatisch gefundenen Geräte ohne Profil oder nur Geräte mit Profil angezeigt werden. Diese Option kann auch über die Befehlsfolge **View** → **All Devices** (Anzeige → Alle Geräte) auf der Menüleiste umgeschaltet werden.

Hinweis: *Die Verbindungsmethode „Durchsuchen" ist die einzige Methode zum Herstellen einer Verbindung mit einem zur Verwendung von DHCP-IP-Adressen konfigurierten Raritan-Gerät.*

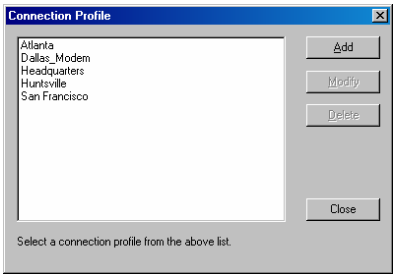
Erstellen neuer Profile

Verbindungsprofile speichern wichtige Informationen zum Raritan-Gerät, z.B. IP-Adresse, angepasste TCP-Ports, bevorzugte Komprimierungseinstellungen und angepasste Sicherheitsschlüssel.

Hinweis: *Wenn Ihr Raritan-Gerät zur Verwendung eines angepassten TCP-Ports (siehe* ***Kapitel 4: Verwaltungsfunktionen, Netzwerkkonfiguration****) oder eines Gruppensicherheitsschlüssels (siehe* ***Kapitel 4: Verwaltungsfunktionen, Sicherheitsekonfiguration****) konfiguriert ist, erstellen Sie zuerst ein Verbindungsprofil, um den Zugriff auf das Gerät zu ermöglichen.*

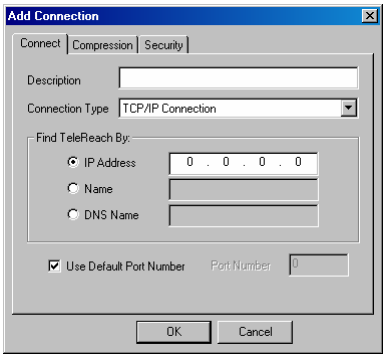
So erstellen Sie ein Verbindungsprofil:

1. Wählen Sie **Connection** → **New Profile** (Verbindung → Neues Profil) auf der Menüleiste, oder klicken Sie auf das Symbol ganz links auf der Symbolleiste. Das Dialogfeld **Connection Profile** (Verbindungsprofil) wird mit einer Liste aller derzeit vorhandenen Verbindungsprofile angezeigt.



2. Klicken Sie auf **Add** (Hinzufügen).
3. Das Dialogfeld **Add Connection** (Verbindung hinzufügen) wird angezeigt. Die Optionen sind auf drei Registerkarten gruppiert: **Connect** (Verbinden), **Compression** (Komprimierung) und **Security** (Sicherheit).

Registerkarte Connect (Verbinden)



- **Description** (Beschreibung)**:** Geben Sie einen Textnamen ein, um das zu konfigurierende Raritan-Gerät leichter zu identifizieren, z.B. „Frankfurter_Rechenzentrum".

- **Connection Type** (Verbindungstyp)**:** Wählen Sie **TCP/IP Connection** (TCP/IP-Verbindung) für eine LAN/WAN-Verbindung oder **Dail-Up Connection** (DFÜ-Verbindung) für eine direkte analoge Modemverbindung mit dem Raritan-Gerät.

Wählen Sie für eine TCP/IP-Verbindung aus, wie RRC Ihr Raritan-Gerät suchen soll:

- **IP Address** (IP-Adresse)**:** RRC sucht nach der IP-Adresse des Raritan-Geräts (siehe **Kapitel 4: Verwaltungsfunktionen**, ***Netzwerkkonfiguration***).
- **Name:** RRC sucht nach dem Namen, der dem Raritan-Gerät bei der Anfangskonfiguration zugewiesen wurde (siehe **Kapitel 4: Verwaltungsfunktionen**, ***Netzwerkkonfiguration***).

Hinweis: *Wenn für IP-Reach dynamische DHCP-Adressen konfiguriert sind, verwenden Sie* ***Find IP-Reach by Name*** *(IP-Reach nach Namen suchen).*

Hinweis: *Der werkseitig voreingestellte Name für jede IP-Reach-Einheit lautet <IP-Reach>. Informationen zum Ändern des Standardnamens einer IP-Reach-Einheit und zur Vergabe eines eindeutigen Namens finden Sie in Kapitel 4.*

- **DNS Name** (DNS-Name)**:** Wenn Sie Ihren DNS-Server zur Auflösung eines DNS-Namens in die dem Raritan-Gerät zugewiesene IP-Adresse konfiguriert haben, verwenden Sie diesen DNS-Namen für den Zugriff auf das Raritan-Gerät.

Für eine DFÜ-Verbindung geben Sie die Wählparameter ein, die RRC zum Herstellen einer Verbindung verwenden soll:

- **Phone Number** (Telefonnummer)**:** Geben Sie alle zusätzlichen Vorwahlen ein, die RRC zum Herstellen einer Verbindung wählen soll (Länder- oder Städtevorwahlziffern, Vorwahlziffern für Amtsleitungen usw.).
- **Modem:** Wählen Sie das in Windows konfigurierte Modem aus, über das RRC eine DFÜ-Verbindung mit Ihrem Raritan-Gerät herstellen soll.

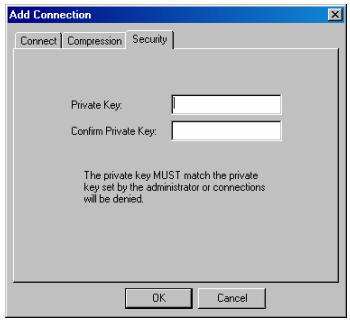
Wählen Sie einen TCP-Port aus:

- **Use Default Port Number** (Standardportnummer verwenden)**:** IP-Reach ist standardmäßig zur Verwendung des TCP-Ports 5000 für die Kommunikation mit RRC konfiguriert. IP-Reach kann bei Bedarf zur Verwendung eines anderen TCP-Ports konfiguriert werden (siehe **Kapitel 4: Verwaltungsfunktionen**, ***Netzwerkkonfiguration***). Deaktivieren Sie in diesem Fall die Option **Use Default Port Number** (Standardportnummer verwenden), und geben Sie den konfigurierten TCP-Port ein.

Registerkarte Compression (Komprimierung)

Die Einstellungen auf der Registerkarte **Compression** (Komprimierung) können über den RRC-Client angepasst werden. Sie sind nicht erforderlich für die Vorkonfiguration im Verbindungsprofil. Wenn Sie diese Einstellungen vorab konfigurieren möchten, lesen Sie hierzu den Abschnitt **Verbindungs- und Videoeigenschaften** in diesem Kapitel.

Registerkarte Security (Sicherheit)



Wenn Sie Ihre IP-Reach-Einheit für einen privaten Gruppenschlüssel konfiguriert haben, geben Sie diesen hier ein, um für die Herstellung einer Verbindung mit dieser IP-Reach-Einheit autorisiert zu werden. Klicken Sie auf **OK**, nachdem Sie die Felder ausgefüllt haben.

Klicken Sie nach Bearbeitung der Bildschirme **Connect** (Verbinden) und **Security** (Sicherheit) auf **OK**, um die Herstellung der Verbindung abzuschließen.

Einrichten einer neuen Verbindung

Zum Herstellen einer Verbindung zu einem vernetzten Raritan-Gerät, doppelklicken Sie auf den entsprechenden Eintrag im RRC-Navigator. Sie werden zur Authentifizierung des Geräts aufgefordert.

Hinweis: *Der Standardbenutzername für die IP-Reach-Anmeldung lautet <admin> und das Kennwort <raritan>. Dieser Benutzer besitzt Administratorrechte. Kennwörter unterliegen der Groß-/Kleinschreibung und müssen genau in der bei ihrer Erstellung verwendeten Schreibweise eingegeben werden. Das Standardkennwort <raritan> muss in Kleinbuchstaben eingegeben werden. Zur Gewährleistung der Sicherheit sollten der Standardbenutzername und das Kennwort so bald wie möglich geändert werden.*

Wird für Ihr IP-Reach-Gerät kein Eintrag im RRC-Navigator angezeigt, folgen Sie den Anweisungen im Abschnitt „Erstellen neuer Profile“ in diesem Kapitel, um ein neues Verbindungsprofil für das IP-Reach-Gerät zu erstellen.

Wenn Probleme beim Herstellen einer Verbindung mit einem Raritan-Gerät auftreten, überprüfen Sie Folgendes:

- **Benutzername/Kennwort:** Für Raritan-Benutzernamen und -Kennwörter muss die Groß-/Kleinschreibung beachtet werden.
- **TCP-Port:** Wenn Sie das Raritan-Gerät zur Verwendung eines nicht standardmäßigen TCP-Ports konfiguriert haben, müssen diese Informationen in das Verbindungsprofil eingegeben werden.
- **Firewalleinstellungen:** Wenn Sie über eine Firewall auf ein Raritan-Gerät zugreifen, muss die Firewall ein- und ausgehende Kommunikation über TCP-Port 5000 (oder den für das Raritan-Gerät konfigurierten angepassten TCP-Port) zulassen.
- **Sicherheitsschlüssel:** Wenn Sie das Raritan-Gerät so konfiguriert haben, dass ein Gruppensicherheitsschlüssel erforderlich ist, muss dieser Schlüssel in das Verbindungsprofil des Geräts eingegeben werden.

Beenden einer Remoteverbindung

Wenn Sie die Verbindung zu einer IP-Reach-Einheit beenden möchten, klicken Sie mit der rechten Maustaste auf den entsprechenden Geräteeintrag im RRC-Navigator und wählen Sie **Disconnect** (Verbindung trennen).

RRC-Symbolleiste und Verknüpfungen

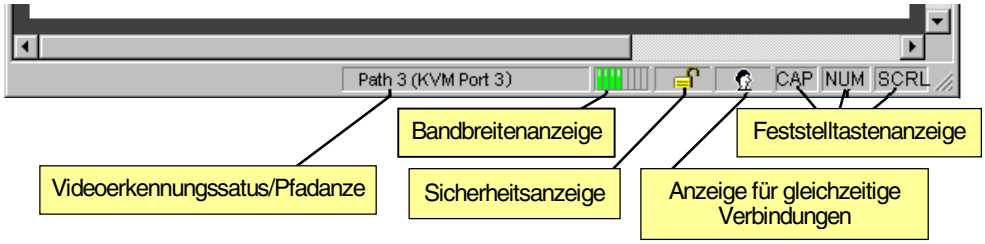
Symbolleiste von Raritan Remote Client

Die RRC-Symbolleiste bietet bequemen Zugriff per Mausklick auf die meisten häufig verwendeten Funktionen und Parameter von Raritan Remote Client.

SCHALTFLÄCHE	SCHALTFLÄCHEN-NAME	ZUGRIFFSTASTE	FUNKTION
	New Profile (Neues Profil)	<Strg+Alt+C>	Erstellt einen neuen Navigator-Eintrag für ein Raritan-Gerät. Die gleiche Funktion bietet die Auswahl von Connection → New Profile (Verbindung à Neues Profil) auf der Menüleiste.
	Connection Properties (Verbindungseigenschaften)	<Strg+Alt+P>	Öffnet das Dialogfeld **Modify Connection Properties** (Verbindungseigenschaften ändern) zur manuellen Anpassung von Bandbreitenoptionen (Verbindungsgeschwindigkeit, Farbtiefe usw.).
	Video Settings (Videoeinstellungen)	Nicht zutreffend	Öffnet das Dialogfeld **Video Settings** (Videoeinstellungen) zur manuellen Anpassung von Videokonvertierungsparametern.
	Synchronize Mouse (Maus synchronisieren)	<Strg+Alt+S>	Erzwingt im Zwei-Cursor-Modus die erneute Ausrichtung des Zielservercursors mit dem Raritan Remote Client-Cursor.
	Refresh Screen (Anzeige aktualisieren)	<Strg+Alt+R>	Aktualisiert den Videobildschirm.
	Auto-sense Video Settings (Videoeinstellungen automatisch erkennen)	<Strg+Alt+A>	Erzwingt die Aktualisierung von Videoeinstellungen (Auflösung, Aktualisierungsfrequenz).
	Enter On-Screen Menu (Bildschirmmenü öffnen)	Nicht zutreffend	Greift auf die Bildschirmbenutzerschnittstelle des verbundenen KVM-Switches zu.
	Exit On-Screen Menu (Bildschirmmenü beenden)	ESC	Deaktiviert die Bildschirmbenutzerschnittstelle des verbundenen KVM-Switches.
	Send Ctrl+Alt+Del (Strg-Alt-Entf senden)	<Strg+Alt+D>	Sendet das Makro „Strg+Alt+Entf“ an den Zielserver.
	Single Cursor Mode (Ein-Cursor-Modus)	<Strg+Alt+X>	Aktiviert den Ein-Cursor-Modus, in dem der Cursor des lokalen PC nicht mehr auf dem Bildschirm angezeigt wird. Drücken Sie <Strg+Alt+X>, um diesen Modus zu beenden.
	Full Screen Mode (Vollbildmodus)	<Strg+Alt+F>	Maximiert die Anzeige des Zielserverdesktops, so dass er auf dem gesamten Bildschirm angezeigt wird.
	Show / Hide Navigator (Navigator ein-/ausblenden)	Nicht zutreffend	Blendet den RRC-Navigator ein bzw. aus.
	Refresh Navigator (Navigator aktualisieren)	Nicht zutreffend	Erzwingt eine Aktualisierung der im RRC-Navigator angezeigten Daten.
	Show / Hide „Browsed“ Devices („Gefundene“ Geräte ein-/ausblenden)	Nicht zutreffend	Blendet die automatisch im Netzwerk identifizierten Raritan-Geräte im RRC-Navigator ein oder aus (Geräte ohne vorkonfigurierte Profile).
	About (Info)	Nicht zutreffend	Zeigt Versionsinformationen zu Raritan Remote Client an.

RRC-Statusleiste

Die **Statusleiste** am unteren Rand des Fenster **Raritan Remote Client** enthält Informationen über den Status Ihrer Remoteverbindungssitzung mit IP-Reach.



Videoerkennungsstatus/Pfadanzeige

Zeigt an, ob eine Videoerkennung stattfindet.

Bandbreitenanzeige

Zeigt an, wie viel der insgesamt verfügbaren Bandbreite zurzeit verwendet wird. Die Einstellung **Connection Speed** (Verbindungsgeschwindigkeit) auf der Registerkarte **Compression** (Komprimierung) des Fensters **Connection Properties** (Verbindungseigenschaften) bestimmt die insgesamt verfügbare Bandbreite.

Sicherheitsanzeige

Zeigt an, ob die aktuelle Remoteverbindung durch Verschlüsselung geschützt ist. Verschlüsselungsanforderungen werden während der Konfiguration des IP-Reach-Geräts festgelegt (siehe **Kapitel 4**). Wenn ein IP-Reach-Gerät auf **No encryption** (Keine Verschlüsselung) oder **SSL Authentication, NO data encryption** (SSL-Authentifizierung, KEINE Datenverschlüsselung) eingestellt ist, wird die Sicherheitsanzeige als geöffnetes Schloss auf der Statusleiste angezeigt. Wenn **SSL authentication, data encryption** (SSL-Authentifizierung, Datenverschlüsselung) oder **SSL authentication, SSL encryption** (SSL-Authentifizierung, SSL-Verschlüsselung) aktiviert ist, wird die Sicherheitsanzeige auf der Statusleiste als geschlossenes Schloss angezeigt.

Anzeige für gleichzeitige Verbindungen

Zeigt an, ob mehrere Remotebenutzer mit demselben IP-Reach-Pfad verbunden sind. Für einen verbundenen Benutzer wird ein Symbol und für mehrere verbundene Benutzer werden zwei Symbole angezeigt.

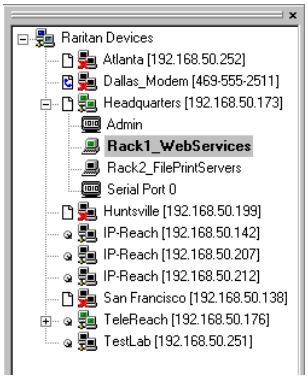
Die Funktion für gleichzeitige Verbindungen kann unter **PC Share Mode** (PC-Freigabemodus) im Fenster **Security Configuration** (Sicherheitskonfiguration) global eingestellt werden (siehe **Kapitel 4**). Für einzelne Benutzer kann diese Funktion mit der Einstellung **Concurrent Access Mode** (Gleichzeitiger Zugriffsmodus) im Fenster **User Account Settings** (Benutzerkonteneinstellungen) aktiviert werden (siehe **Kapitel 4**).

Feststelltastenanzeige

Zeigt den Status des aktuellen Zielservers hinsichtlich der Aktivierung der Feststelltaste, Num-Feststelltaste und Rollen-Taste an. Wenn diese Tasten auf dem angezeigten Zielserver aktiviert sind, wird dieser Status auf der Statusleiste angezeigt.

Remote-KVM-Konsolensteuerung

Nachdem Sie anhand des RRC-Navigators eine Verbindung zu einer IP-Reach-Einheit hergestellt haben (siehe hierzu den vorhergehenden Abschnitt **Einrichten einer Verbindung**), wird der der IP-Reach-Einheit entsprechende Navigator-Eintrag erweitert und zeigt alle für den Remotezugriff aktivierte Ports des IP-Reach-Geräts an.

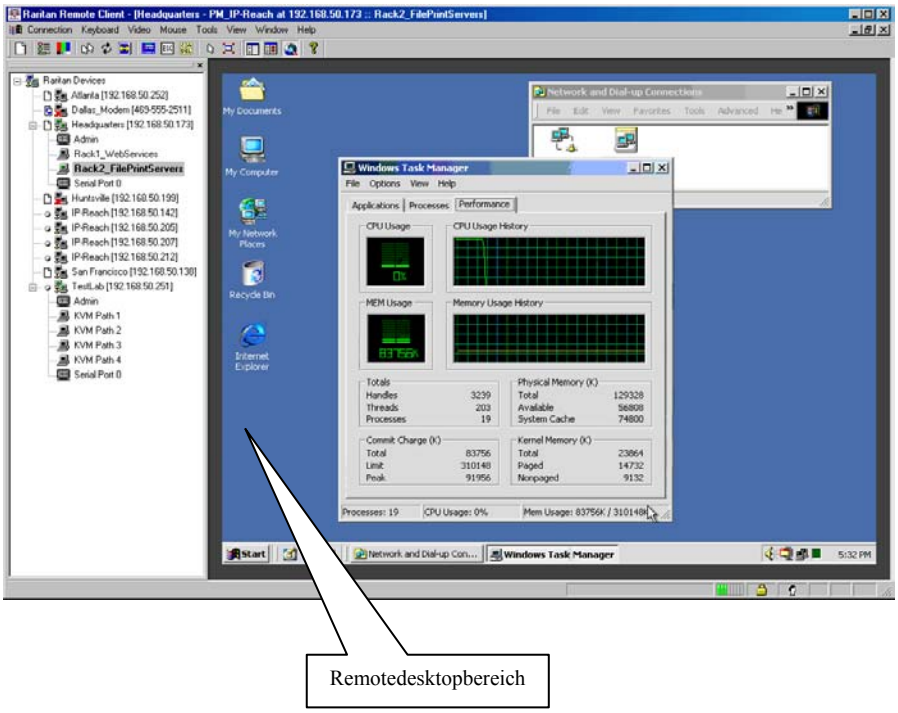


Zum Herstellen einer Remote-KVM-Konsolenverbindung doppelklicken Sie auf den KVM-Pfad, den Sie steuern möchten.

Nachdem die Verbindung hergestellt wurde, zeigt IP-Reach eine Echtzeit-Videoausgabe des mit dem KVM-Port des IP-Reach Geräts verbundenen KVM-Switches oder Servers an. Diese Videoausgabe wird entsprechend den vom Administrator festgelegten Konfigurationseinstellungen komprimiert und verschlüsselt (siehe **Kapitel 4**).

Sobald die Verbindung zu einem KVM-Switch oder einem Server hergestellt wurde, können Sie die KVM-Konsole nun wie bei der lokalen Arbeit am KVM-Switch oder Server vollständig auf niedriger Ebene steuern.

Wenn sich Ihr Cursor im Remotedesktopbereich von RRC befindet, werden Mausbewegungen und -klicks an den verbundenen KVM-Switch oder Remoteserver übertragen.



Ein-Cursor-Modus/Zwei-Cursor-Modus

Bei der Remoteanzeige eines Zielservers mit Zeigegerät werden im Remotedesktopbereichs des Fensters **Raritan Remote Client** zwei Cursor angezeigt. Der Raritan Remote Client-Cursor für das Betriebssystem, auf dem RRC ausgeführt wird, ist dem Cursor des Zielservers aufgrund der digitalen Verzögerung während der Bewegung leicht vorgelagert.

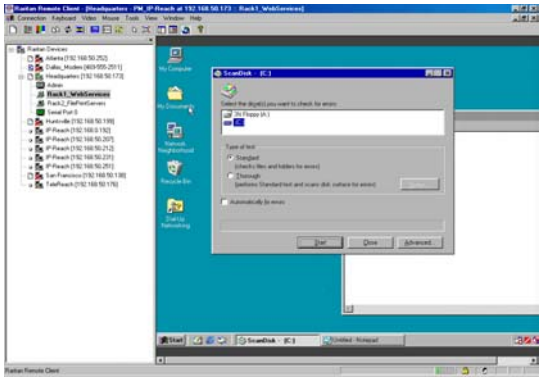
Bei schnellen LAN-Verbindungen ziehen manche Benutzer es vor, den Raritan Remote Client-Cursor zu deaktivieren und nur den Cursor des Zielservers anzuzeigen. Verwenden Sie die Tastenkombination <**Strg+Alt+X**>, um zwischen den beiden Modi umzuschalten, oder klicken Sie auf der RRC-Symbolleiste auf das Symbol **Single Mouse Pointer** (Ein Cursor).

Hinweis: *Klicken Sie zum Verbessern der Cursorausrichtung im Zwei-Cursor-Modus auf die Schaltfläche* ***Synchronize Mouse*** *(Maus synchronisieren) der RRC-Symbolleiste oder drücken Sie die Tastenkombination <**Strg+Alt+S**>. Dadurch wird eine erneute Ausrichtung der beiden Cursor erzwungen. Wenn Sie die Anweisungen zum Konfigurieren von Zielservern in Kapitel 2 genau befolgt haben und die Cursor dennoch nicht synchronisiert sind, klicken Sie auf der RRC-Symbolleiste auf die Schaltfläche* ***Auto-Sense Video*** *(Videoeinstellungen automatisch erkennen) .*

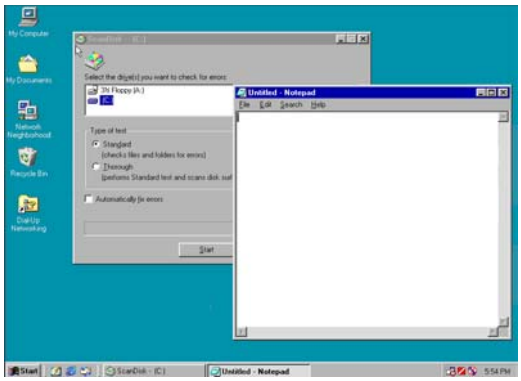
Vollbildmodus

Der Vollbildmodus von Raritan Remote Client maximiert die für RRC verfügbare Anzeige des Remotedesktop, indem Fensterrahmen, Symbolleisten, Statusleisten und der RRC-Navigator entfernt werden.

Dieser Modus eignet sich besonders für die Anzeige eines Zielservers, dessen Auflösung gleich oder größer als die Videoauflösungseinstellung auf dem PC ist, auf dem RRC ausgeführt wird, z.B. beim Anzeigen eines Servers mit der Auflösung 1024x768 auf einem PC mit der Auflösung 1024x768.



Standardansicht



Anzeige im Vollbildmodus

Klicken Sie zum Aktivieren bzw. Deaktivieren des Vollbildmodus auf der RRC-Symbolleiste auf das Vollbildmodussymbol (oder drücken Sie <**Strg+Alt+F**>). Zum Beenden des Vollbildmodus drücken Sie die Tastenkombination <**Strg+Alt+F**>.

Auswählen von Servern anhand eines KVM-Switches

Für den Zugriff per Mausklick auf die vom KVM-Switch bereitgestellte Bildschirmbenutzerschnittstelle stehen zwei Schaltflächen zur Verfügung. Die Schaltflächen **Enter OSUI** (Bildschirmbenutzerschnittstelle öffnen) und **Exit OSUI** (Bildschirmbenutzerschnittstelle schließen) sollen die Verwendung von IP-Reach in Verbindung mit KVM-Switches vereinfachen.

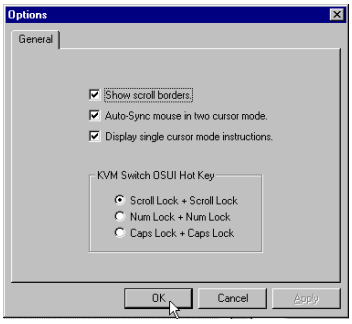
	Bildschirmbenutzerschnittstelle öffnen
	Bildschirmbenutzerschnittstelle schließen

Führen Sie die unten angegebenen Schritte aus, um RRC für die Interoperabilität mit den KVM-Switches zum Öffnen und Schließen der entsprechenden Benutzerschnittstellen zu konfigurieren. Sobald IP-Reach auf die Zugriffstaste Ihres KVM-Switches konfiguriert wurde, können die Zielserver anhand der bereits erwähnten zwei Schaltflächen auf der RRC-Symbolleiste ausgewählt werden.

Hinweis: *Um auf die KVM-Bildschirmbenutzerschnittstelle zuzugreifen, können Remotebenutzer auch einfach auf der Tastatur des Remote-PC die KVM-Switch-Zugriffstaste eingeben. Dies gilt sowohl für Raritan- als auch für nicht Raritan-KVM-Produkte.*

Damit die Switching-Symbole von RRC verwendet werden können, muss für IP-Reach die Zugriffstaste der Bildschirmbenutzerschnittstelle des verbundenen KVM-Switch eingerichtet sein. Hierbei handelt es sich um einen einmaligen Installationsvorgang, der nur wiederholt werden muss, wenn die Belegung der Zugriffstaste des KVM-Switches geändert wird.

1. Als Zugriffstaste für die Bildschirmbenutzerschnittstelle können Sie die <**Rollen-Taste**>, die <**Num-Feststelltaste**> oder die <**Feststelltaste**> verwenden. Legen Sie eine dieser Zugriffstasten für die Aktivierung der Bildschirmbenutzerschnittstelle Ihres KVM-Switches fest. Falls Sie keine Taste festlegen, können Sie zu diesem Zweck auch ein Tastaturmakro (siehe nächster Abschnitt) erstellen.
2. Wählen Sie auf der RRC-Menüleiste **Tools** → **Options** (Extras → Optionen).



4. Wählen Sie die entsprechende Zugriffstaste, die die Bildschirmbenutzerschnittstelle des verbundenen KVM-Switches aktiviert.
5. Klicken Sie zum Fortfahren auf **OK**.

Tastaturmakros

Mit RRC können benutzerdefinierte Tastaturmakros erstellt werden, um definierte Tastenfolgen an den mit IP-Reach verbundenen Remoteserver oder KVM-Switch zu senden. Mit dieser Funktion können Benutzer Tastaturanschläge an Remoteserver senden, die anderenfalls von dem RRC ausführenden Computer willkürlich interpretiert würden.

Die Tastaturmakrofunktion von IP-Reach gewährleistet, dass für den Zielserver bestimmte Tastenkombinationen an den Zielserver gesendet und nur von diesem interpretiert werden.

Makro „Strg+Alt+Entf“

Aufgrund der häufigen Verwendung dieser Tastenkombination ist ein Makro „Strg+Alt+Entf“ in Raritan Remote Client vorprogrammiert und dient zur Veranschaulichung der Leistungsfähigkeit von Tastaturmakros.

	Send Ctrl+Alt+Del (Strg-Alt-Entf senden)	<Strg+Alt+D>	Sendet das Makro „Strg+Alt+Entf“ an den Zielserver.

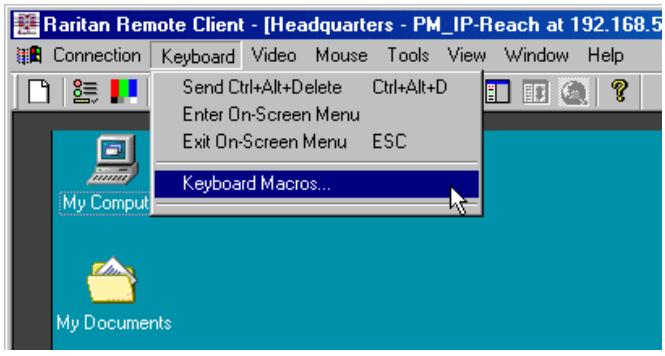
Wenn Sie auf der RRC-Symbolleiste auf das Symbol **Strg+Alt+Entf** klicken, wird diese Tastenfolge an den Server oder KVM-Switch gesendet, mit dem Sie zurzeit verbunden sind. Wenn Sie aber bei der Verwendung von RRC die Tastenkombination **Strg+Alt+Entf** drücken, wird diese Eingabe aufgrund der Struktur des Betriebssystems Windows zunächst von Ihrem eigenen PC interpretiert und nicht wie gewünscht an den Zielserver gesendet.

Erstellen eines Tastaturmakros

Die folgenden Anweisungen beschreiben ausführlich die Schritte, die zum Erstellen eines Tastaturmakros für den Windows-Befehl **Alle Fenster minimieren/Desktop anzeigen** erforderlich sind.

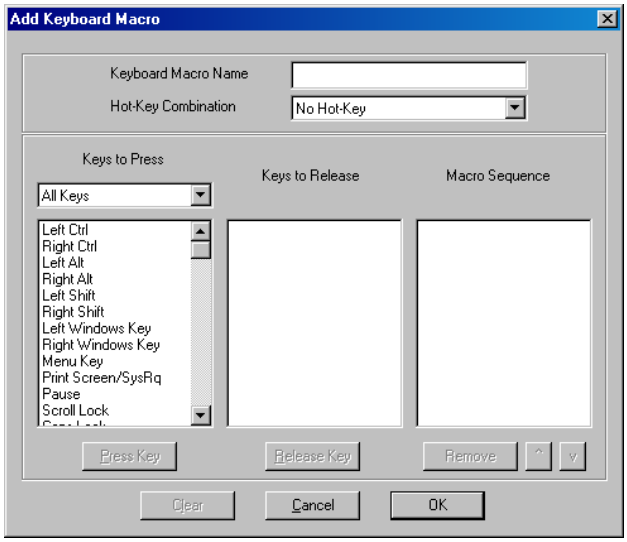
Wenn Sie in Windows die Tastenkombination <**Windows+D**> drücken, werden alle Programmfenster minimiert. Wenn Sie jedoch über RRC mit einem Zielserver verbunden sind, ist ein Tastaturmakro die einzige Möglichkeit, um diese Aufgabe auf dem Zielserver auszuführen. Dies ist darauf zurückzuführen, dass die Tastenkombination <**Windows+D**> auf Ihrem eigenen Client-PC interpretiert und ausgeführt wird, anstatt den Befehl wie beabsichtigt an den Zielserver zu senden.

1. Wählen Sie auf der RRC-Menüleiste **Keyboard** → **Keyboard Macros** (Tastatur → Tastaturmakros).

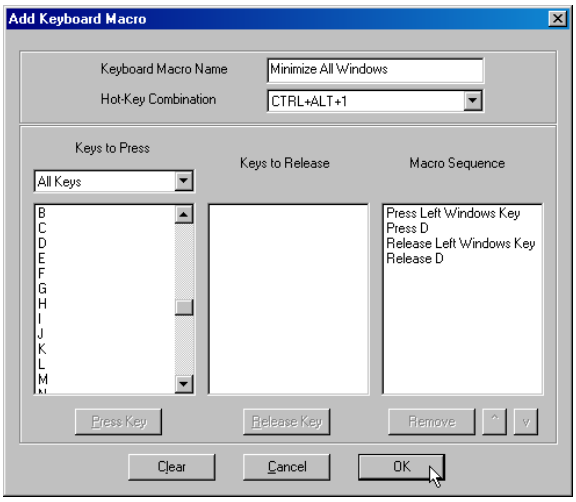


2. Klicken Sie im Dialogfeld **Keyboard Macros** (Tastaturmakros) auf **Add** (Hinzufügen).

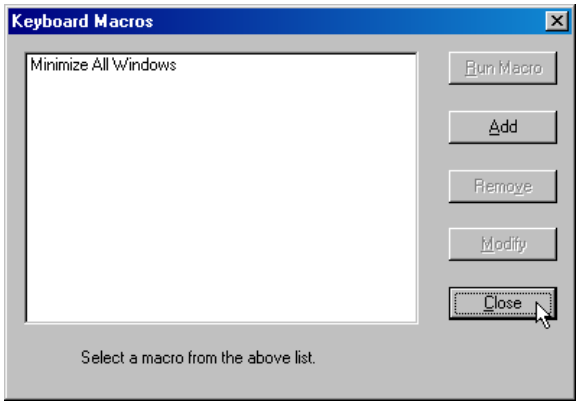
3. Das Dialogfeld **Add Keyboard Macro** (Tastaturmakro hinzufügen) wird angezeigt.



4. Erstellen Sie das Tastaturmakro durch Bearbeiten aller Felder im Fenster **Add Keyboard Macro** (Tastaturmakro hinzufügen) in der unten angegebenen Reihenfolge. Klicken Sie anschließend auf **OK**.
   a. Geben Sie einen Namen im Feld **Keyboard Macro Name** (Name des Tastaturmakros) ein, der nach erfolgreicher Erstellung des Tastaturmakros auf der RRC-Menüleiste angezeigt wird. In dem hier genannten Beispiel geben Sie den Namen „Alle Fenster minimieren“ ein.
   b. **Optional:** Geben Sie eine Tastenkombination in das Feld **Hot-Key Combination** (Zugriffstastenkombination) ein, mit der Sie das Makro von Ihrer Tastatur leicht ausführen können, während RRC aktiv ist. Für das Beispiel „Alle Fenster minimieren“ wählen Sie **<Strg+Alt+1>**.
   c. Wählen Sie im Auswahlfeld **Keys to Press** (Zu betätigende Tasten) die einzelnen Tasten, für die Sie Tastenanschläge emulieren möchten, in der entsprechenden Reihenfolge aus, und klicken Sie nach jeder Auswahl auf [**Press Key**] (Taste drücken). Jede ausgewählte Taste wird im Auswahlfeld **Keys to Release** (Freizugebende Tasten) in der Mitte des Dialogfelds angezeigt.
      - In unserem Beispiel „Alle Fenster minimieren“ fordern wir das Senden von zwei Tasten an: die **<Windows>**-Taste und die **<D>**-Taste.
   d. Wählen Sie im Auswahlfeld **Keys to Release** (Freizugebende Tasten) die einzelnen Tasten, für die Sie Tastenanschläge emulieren möchten, in der entsprechenden Reihenfolge aus, und klicken Sie nach jeder Auswahl auf **Release Key** (Taste freigeben).
      - In unserem Beispiel „Alle Fenster minimieren“ sollen beide gedrückte Tasten auch freigegeben werden.
   e. Prüfen Sie im Feld **Macro Sequence** (Makrosequenz), dessen Inhalt automatisch erzeugt wird, ob der Inhalt die gewünschte Tastenfolge genau widerspiegelt. Passen Sie den Inhalt und die Reihenfolge des Makros, falls erforderlich, mit der Schaltfläche **Remove** (Entfernen) und den Pfeilschaltflächen an.



5. Nachdem Sie auf **OK** geklickt haben, wird das Dialogfeld **Keyboard Macros** (Tastaturmakros) mit Ihrem neuen Tastaturmakro geöffnet.



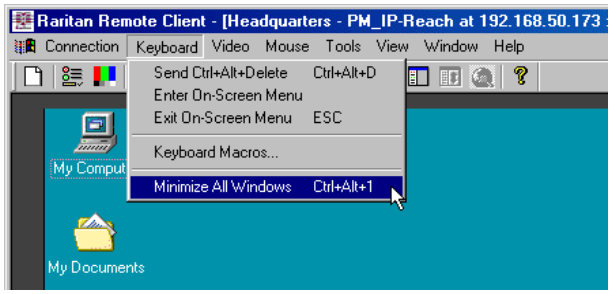
6. Klicken Sie auf **Close** (Schließen), um die Bearbeitung des Tastaturmakros abzuschließen.

Ausführen eines Tastaturmakros

Sobald ein Makro erstellt wurde, kann es über die RRC-Menüleiste oder mit der Zugriffstastenkombination ausgeführt werden, sofern eine solche Kombination beim Erstellungsvorgang definiert wurde.

Aktivierung über die Menüleiste

Nach dem Erstellen eines Makros wird es im Menü **Keyboard** (Tastatur) auf der RRC-Menüleiste angezeigt. Klicken Sie zum Ausführen Ihres neuen Tastaturmakros auf den Eintrag.



Aktivierung über die Zugriffstasten

Alternativ kann ein erstelltes Makro unter Verwendung von RRC durch Drücken der Zugriffstaste, die Sie dem Makro (optional) zugewiesen haben, ausgeführt werden. In dem obigen Beispiel „Alle Fenster minimieren“ kann ein Benutzer die Tasten <**Strg+Alt+1**> gleichzeitig drücken und mit RRC die Tastenkombination <**Windows+D**> an den Zielserver senden.

Verbindungs- und Videoeigenschaften

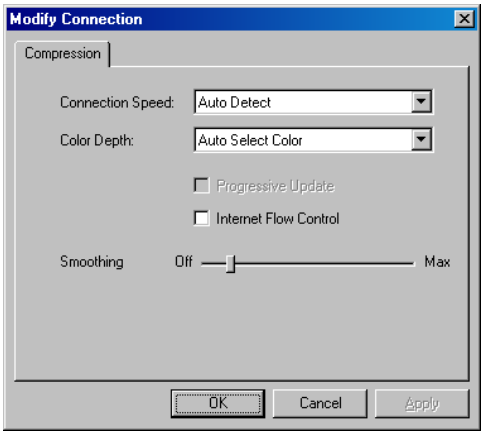
Die dynamischen Videokomprimierungsalgorithmen von IP-Reach gewährleisten die Verwendbarkeit der KVM-Konsole unter variierenden Bandbreitenbeschränkungen. Im Gegensatz zu Konkurrenzprodukten optimiert IP-Reach seine KVM-Ausgabe nicht nur für die LAN-Nutzung, sondern auch für die Nutzung über ein WAN und DFÜ. Durch dynamische Anpassung der Farbtiefe und Beschränkung der Videoausgabe stellt IP-Reach für jede Bandbreite ein optimales Gleichgewicht zwischen Videoqualität und Systemreaktion bereit.

RRC-Hauptbenutzer sollten mit den folgenden einstellbaren Parametern in den Dialogfeldern **Connection Properties** (Verbindungseigenschaften) und **Video Settings** (Videoeinstellungen) sowie den Auswirkungen jeder Einstellung vertraut sein. Diese Einstellungen können in unterschiedlichen Umgebungen den jeweiligen Anforderungen entsprechend optimiert werden.

Connection Properties (Verbindungseigenschaften)

	Connection Properties (Verbindungseigenschaften)	<Strg+Alt+P>	Öffnet das Dialogfeld **Modify Connection Properties** (Verbindungseigenschaften ändern) zur manuellen Anpassung von Bandbreitenoptionen (Verbindungsge-schwindigkeit, Farbtiefe usw.).

Wählen Sie für den Zugriff auf das Dialogfeld **Connection Properties** (Verbindungseigenschaften) entweder **Connection → Connection Properties** (Verbindung → Verbindungseigenschaften) auf der RRC-Menüleiste oder klicken Sie auf **Connection Properties** (Verbindungseigenschaften) auf der RRC-Symbolleiste.



Connection Speed (Verbindungsgeschwindigkeit)

Mit dem Auswahlfeld **Connection Speed** (Verbindungsgeschwindigkeit) können Benutzer die von IP-Reach verwendete Netzwerkbandbreite auf den definierten Wert beschränken. IP-Reach erkennt die verfügbare Bandbreite in der Regel automatisch. Anhand der Einstellung **Connection Speed** (Verbindungsge-schwindigkeit) kann IP-Reach jedoch manuell über eine Bandbreitenbeschränkung informiert werden. Dabei passt IP-Reach sein Verhalten entsprechend an und unternimmt keinen Versuch, mehr als die verfügbare Bandbreite in Anspruch zu nehmen.

Color Depth (Farbtiefe)

Für die meisten Verwaltungsaufgaben (Überwachung, erneute Konfiguration von Servern usw.) benötigen Serveradministratoren das von den modernen Videografikkarten bereitgestellte vollständige 24-Bit- oder 32-Bit-Farbspektrum nicht. Durch die Übertragung solch hoher Farbtiefen werden enorme Mengen wertvoller Netzwerkbandbreite verschwendet.

IP-Reach kann die an Remotebenutzer übertragene Farbtiefe dynamisch anpassen, um die Verwendbarkeit unter allen Bandbreitenbeschränkungen zu maximieren.

- **Progressive Update** (Progressive Aktualisierung)**:** Die äußerst innovative IP-Reach-Funktion der progressiven Aktualisierung kann die Verwendbarkeit in Umgebungen mit beschränkter Bandbreite verbessern. Wenn **Progressive Update** (Progressive Aktualisierung) aktiviert ist, sendet IP-Reach zunächst ein Bild des Remotedesktops mit geringeren Farbtiefen und liefert anschließend entsprechend der verfügbaren Bandbreite Bilder mit höherer Farbtiefe.

  Diese Option ist mit dem bekannten WWW-Prinzip „interlaced GIF“ vergleichbar.

Hinweis: *Wenn die Farbtiefe auf die Standardeinstellung* ***Auto Select Color*** *(Farbe automatisch auswählen) eingestellt ist, wird* ***Progressive Update*** *(Progressive Aktualisierung) automatisiert. IP-Reach aktiviert/deaktiviert die progressive Aktualisierung nach Bedarf, d.h., für schnelle Verbindungen wird die Funktion deaktiviert, und für langsame Verbindungen wird sie aktiviert.*

Internet Flow Control (Internetflusssteuerung)

Viele Links des öffentlichen WAN sind nicht prognostizierbar. Über das öffentliche Internet gesendete Pakete kommen an ihrem Ziel nicht unbedingt in der Reihenfolge an, in der sie gesendet wurden. Wenn Sie IP-Reach über ein nicht prognostizierbares öffentliches WAN verwenden (insbesondere in internationalen Szenarien), können Sie durch Aktivieren des Kontrollkästchens **Internet Flow Control** (Internetflusssteuerung) sicherstellen, dass von IP-Reach übertragene Pakete in der korrekten Reihenfolge von RRC empfangen und rekonstruiert werden.

Smoothing (Glättung)

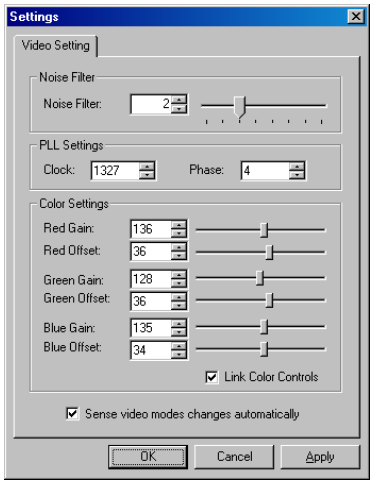
Mit der Videoeinstellung **Smoothing** (Glättung) können Sie IP-Reach die für die Übertragung relevanten Farbstufenveränderungen mitteilen. Von der Hauptfarbe abweichende Videopixel werden ungefähren Farbwerten zugewiesen, um die belegte Bandbreite und das übertragene Videorauschen zu reduzieren. Zu hohe Glättungsebenen können zu ungenauen Farben führen, und zu niedrige Einstellungen erfordern eine höhere Bandbreite und Verarbeitungsleistung.

Video Settings (Videoeinstellungen)

	Video Settings (Videoeinstellungen)	Nicht zutreffend	Öffnet das Dialogfeld **Video Settings** (Videoeinstellungen) zur manuellen Anpassung von Videokonvertierungsparametern.

Wählen Sie für den Zugriff auf das Dialogfeld **Video Settings** (Videoeinstellungen) entweder **Video → Video Settings** (Video → Videoeinstellungen) aus der RRC-Menüleiste, oder klicken Sie auf die Schaltfläche **Connection Properties** (Verbindungseigenschaften) in der RRC-Symbolleiste.

Die meisten Einstellungen in diesem Dialogfenster werden durch eine Farbkalibrierung (wie im folgenden Abschnitt beschrieben) oder durch manuelle Einstellung von IP-Reach auf die automatische Erkennung der Videoeinstellungen aktualisiert (wählen Sie hierzu auf der RRC-Menüleiste **Video → Auto-sense Video Settings** [Video Videoeinstellungen automatisch erkennen]). Für Hauptbenutzer ist das Verständnis dieser Einstellungen jedoch hilfreich.



Noise Filter (Rauschfilter)

Die Videoausgabe von Grafikkarten wird analog übertragen und ist für elektrische und Interferenzstörungen anfällig. Durch die verbesserte Schaltung von IP-Reach können diese kleinen, falschen und unbeabsichtigten Signalabweichungen herausgefiltert werden und somit die Bildqualität und Bandbreitennutzung optimiert werden.

Höher: Die Rauschfiltereinstellungen weisen IP-Reach an, nur dann ein Variantenpixel der Videoausgabe zu übertragen, wenn bei einem Vergleich mit den Nachbarpixeln eine starke Farbabweichung vorliegt. Eine zu hohe Einstellung des Schwellwerts kann jedoch zu einer unbeabsichtigten Filterung von gewünschten Bildschirmänderungen führen.

Niedriger: Die Rauschfiltereinstellungen weisen IP-Reach an, die meisten Pixeländerungen zu übertragen. Eine zu niedrige Einstellung des Schwellwerts kann zu einer höheren Bandbreitennutzung führen.

Hinweis: *Niedrigere Rauschfiltereinstellungen (ca. 1 bis 4) werden empfohlen. Höhere Einstellungen verhindern zwar die unnötige Übertragung von falschen Farbvariationen, sie führen u.U. aber dazu, dass echte und beabsichtigte kleine Änderungen eines Videobilds nicht übertragen werden.*

Analog/Digital-Einstellungen:

Die folgenden Parameter sollten möglichst von IP-Reach automatisch erkannt werden (wählen Sie auf der RRC-Menüleiste die Befehle **Video → Auto-sense Video Settings** [Video → Videoeinstellungen automatisch erkennen]). Sie werden an dieser Stelle kurz beschrieben.

- **PLL Settings** (PLL-Einstellungen)**:** Wenn das Videobild extrem verschwommen oder unscharf wirkt, können die PLL-Einstellungen für die Uhr und die Phase so gewählt werden, dass auf dem aktiven Zielserver ein besseres Bild angezeigt wird.
  - **Clock** (Uhr)**:** Dies ist ein horizontaler Synchronisierungsteiler zum Erzeugen der Pixeluhr. Er steuert, wie schnell Videopixel auf dem Videobildschirm angezeigt werden. Änderungen an den Uhreinstellungen führen zu einer horizontalen Streckung oder Stauchung des Videobilds. Als Einstellung werden ungerade Zahlen empfohlen.
  - **Phase:** Die Phasenwerte liegen zwischen 0 und 31 und werden zyklisch durchlaufen. Stoppen Sie bei dem Phasenwert, der das beste Videobild für den aktiven Zielserver ergibt.
- **Color Settings** (Farbeinstellungen)**:** Sie können sich die Verstärkungssteuerung als Kontrasteinstellung vorstellen. Die Offsetsteuerung ist mit der Helligkeitseinstellung vergleichbar.
  - **Red Gain** (Rot-Verstärkung)**:** Steuert die Verstärkung des roten Signals.
  - **Red Offset** (Rot-Offset)**:** Steuert die Vorspannung des roten Signals.
  - **Green Gain** (Grün-Verstärkung)**:** Steuert die Verstärkung des grünen Signals.
  - **Green Offset** (Grün-Offset)**:** Steuert die Vorspannung des grünen Signals.
  - **Blue Gain** (Blau-Verstärkung)**:** Steuert die Verstärkung des blauen Signals.
  - **Blue Offset** (Blau-Offset)**:** Steuert die Vorspannung des blauen Signals.
  - **Link Color Controls** (Farbsteuerelemente verknüpfen)**:** Verknüpft alle Verstärkungsschieberegler und alle Offset-Verschieberegler, d.h., wenn der Verstärkungsregler einer Farbe verstellt wird, bewegen sich alle Verstärkungsregler, und wenn der Offset-Regler einer Farbe verstellt wird, bewegen sich alle Offset-Regler.
- **Sense video mode changes automatically** (Videomodusänderungen automatisch erkennen)**:** Legt fest, ob IP-Reach das an RRC gesendete Videobild jedes Mal automatisch aktualisiert, wenn eine Änderung der Videoauflösung oder Aktualisierungsfrequenz auf dem Zielserver erkannt wird.

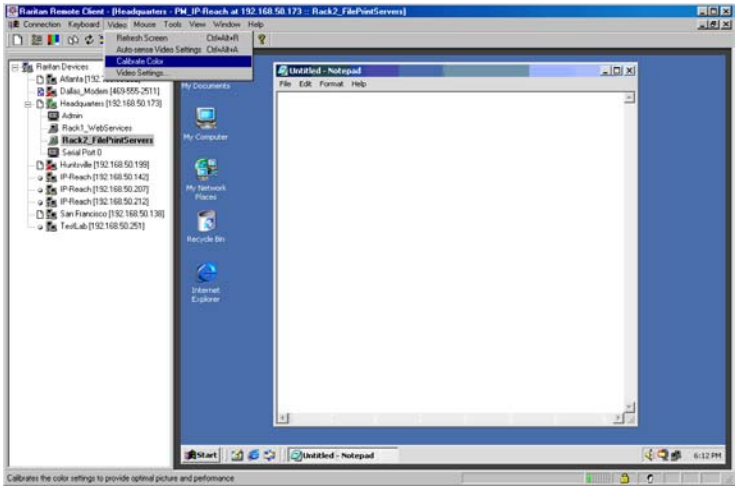
Farbkalibrierung

Bei der automatischen Farbkalibrierung werden die Farbeinstellungen von IP-Reach angepasst, um überflüssiges Farbrauschen und überflüssige Daten während der Digitalisierung von Videobildern zu reduzieren. Durch diese Datenoptimierung wird die Leistung des IP-Reach-Geräts, insbesondere die Farbgenauigkeit, verbessert.

Die Farbkalibrierung, die sehr leicht durchzuführen ist, sollte vorgenommen werden, wenn die Farbstufen (Farbton, Helligkeit, Sättigung) der übertragenen Videobilder ungenau erscheinen. Da die Farbeinstellungen von IP-Reach beim Wechseln zwischen Zielservern unverändert bleiben, gilt eine einmalige Farbkalibrierung auf einem repräsentativen Zielserver für alle verbundenen Zielserver.

So führen Sie die Farbkalibrierung aus:

1. Öffnen Sie auf einem beliebigen Server mit grafischer Benutzeroberfläche eine Remote-KVM-Verbindung.
2. Stellen Sie sicher, dass der Desktop des Zielservers zu mindestens 15 % mit einer einheitlich weißen Farbe belegt ist. Hierzu können Sie einfach die Editoranwendung öffnen und die Fenstergröße maximieren.



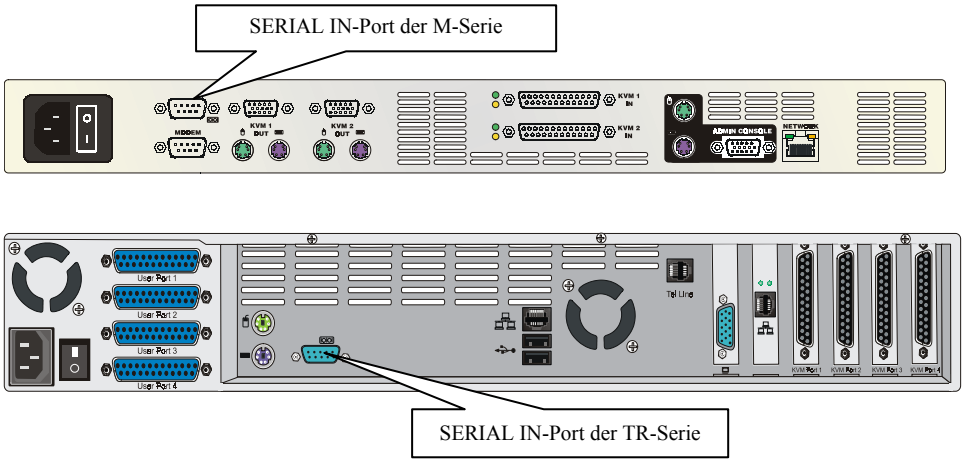
3. Wählen Sie auf der RRC-Menüleiste **Video → Calibrate Color** (Video → Farbe kalibrieren), um die Farbkalibrierung auszuführen.

Serielle Remotesteuerung

Neben dem Remote-KVM-Konsolenzugriff bietet IP-Reach Benutzern außerdem bequemen Zugang zu einer seriellen Konsole über einen Webbrowser. An den seriellen Eingangsport SERIAL IN auf der Rückseite von IP-Reach lässt sich jede beliebige Konsole, die die VT100-Emulation unterstützt, anschließen. Auf diese Konsole kann dann mit Raritan Remote Client zugegriffen werden.

Physische Anschlüsse

Der serielle Eingangsport SERIAL IN auf der Rückseite von IP-Reach ist ein DB9-Stecker mit einem RS-232-DTE-Ausgangspin.

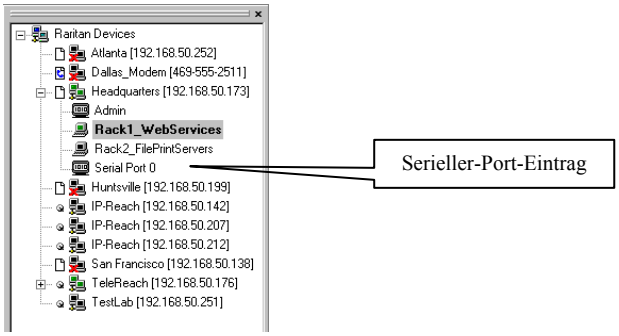


Verwenden Sie zum Anschließen Ihres seriellen Geräts an den seriellen Eingangsport SERIAL IN von IP-Reach Folgendes:

- Ein serielles Durchsteckkabel zum Anschließen von DCE-Konsolen
- Ein serielles Null-Modem-Kabel zum Anschließen von DTE-Konsolen

Remoteverbindung

Zum Herstellen einer Remoteverbindung zur seriellen Konsole, die am seriellen Eingangsport SERIAL IN von IP-Reach angeschlossen ist, doppelklicken Sie auf den seriellen Pfadeintrag, der auf dem RRC-Navigator angezeigt wird. Zugriffsberechtigungen für den seriellen Port können in den Administrationsmenüs festgelegt werden (siehe **Kapitel 4**).



Es wird ein Terminalfenster geöffnet, das die Konsolenausgabe des mit IP-Reach verbundenen seriellen Geräts anzeigt. Das Symbol neben dem seriellen Porteintrag im RRC-Navigator wird grün angezeigt.

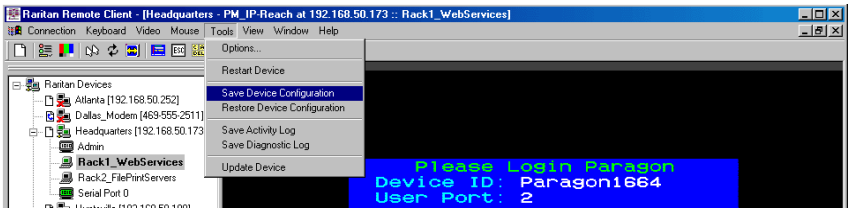
Hinweis: *Der serielle IP-Reach-Konsolenzugriff unterstützt nur die VT100-Terminalemulation. Überzeugen Sie sich von der ordnungsgemäßen Konfiguration Ihres seriellen Geräts, bevor Sie eine Verbindung mit IP-Reach herstellen.*

Ändern serieller Einstellungen

Sie können die seriellen Terminaleinstellungen, wie Baudrate, Parität und Stoppbits, die IP-Reach für die Kommunikation mit Ihrem seriellen Gerät verwendet, ändern. Klicken Sie dazu mit der rechten Maustaste auf den seriellen Porteintrag im RRC-Navigator und wählen Sie aus dem Menü die Option **Serial Parameters** (Serielle Parameter). Klicken Sie anschließend auf **OK**.

Remotegeräteadministration

Wenn Sie sich bei IP-Reach als Benutzer mit Administratorrechten angemeldet haben, können Sie zahlreiche wichtige Geräteadministrationsaufgaben remote ausführen.



Konfigurationsmenüs

Ein Administratorbenutzer kann durch Doppelklicken auf den Porteintrag „Admin“ eines im RRC-Navigator angezeigten IP-Reach-Geräts auf die Konfigurationsmenüs von IP-Reach auf niedrigster Ebene zugreifen (ausführliche Erläuterungen dazu finden Sie in Kapitel 4).

Firmwareaktualisierung

Remotefirmwareaktualisierungen können durch Auswahl von **Tools → Update Device** (Extras → Gerät aktualisieren) auf der RRC-Menüleiste ausgeführt werden. Sofern verfügbar, fordert RRC Sie zur Auswahl einer Raritan-Firmwaredistributionsdatei (*.RFP-Format) in der Raritan-Website (www.raritan.com) auf. Lesen Sie vor dem Durchführen einer Aktualisierung alle Anweisungen in den Firmwaredistributionen.

Geräteneustart

Administratorbenutzer können IP-Reach-Einheiten durch Auswahl von **Tools → Restart Device** (Extras → Gerät neu starten) auf der RRC-Menüleiste neu starten.

Sicherung und Wiederherstellung der Gerätekonfiguration

Durch Auswählen von **Tools → Save Device Configuration** (Extras → Gerätekonfiguration speichern) und **Tools → Restore Device Configuration** (Extras → Gerätekonfiguration wiederherstellen) auf der RRC-Menüleiste können Administratorbenutzer vollständige IP-Reach-Konfigurationen auf ihre lokale Computer zu Archivierungszwecken herunter- und hochladen.

Protokolldateien

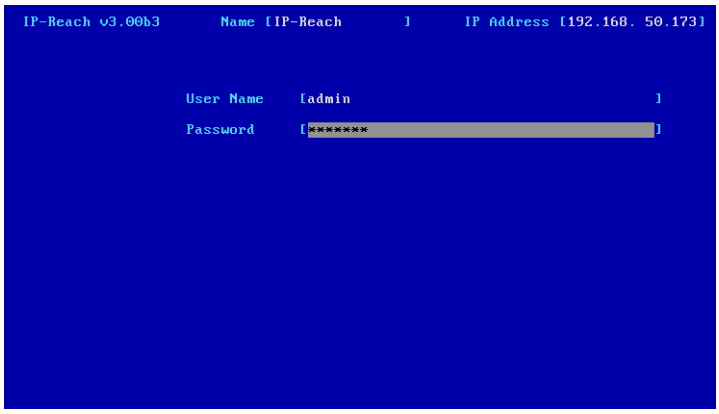
IP-Reach bietet ausführliche Aktivitätsprotokolle zu Problembehandlungszwecken. Diese Protokolle können zum Anzeigen, Erstellen von Berichten und zur Analyse auf Ihren lokalen Computer heruntergeladen werden. Wählen Sie auf der RRC-Menüleiste **Tools → Save Activity Log** (Extras → Aktivitätsprotokoll speichern) oder **Tools → Save Diagnostic Log** (Extras → Diagnoseprotokoll laden).

Kapitel 4: Verwaltungsfunktionen

Zugriff auf die Verwaltungsfunktionen

Verwenden Sie für den Zugriff und zum Ausführen der Verwaltungsfunktionen die lokale Verwaltungskonsole oder die Remoteverwaltung. Nur Administratoren (d.h. Benutzer mit Administratorrechten) können auf die Verwaltungsmenüs von IP-Reach zugreifen.

Lokale Verwaltungskonsole



Schalten Sie das IP-Reach-Gerät mit dem Netzschalter auf der Rückseite des Geräts auf „ON“ (EIN).

Hinweis: *Der Standardbenutzername für die IP-Reach-Anmeldung lautet <admin> und das Kennwort <raritan>. Dieser Benutzer besitzt Administratorrechte.*

Kennwörter unterliegen der Groß-/Kleinschreibung und müssen genau in der bei ihrer Erstellung verwendeten Schreibweise eingegeben werden. Das Standardkennwort <raritan> muss in Kleinbuchstaben eingegeben werden.

Zur Gewährleistung der Sicherheit sollten der Standardbenutzername und das Kennwort so bald wie möglich geändert werden.

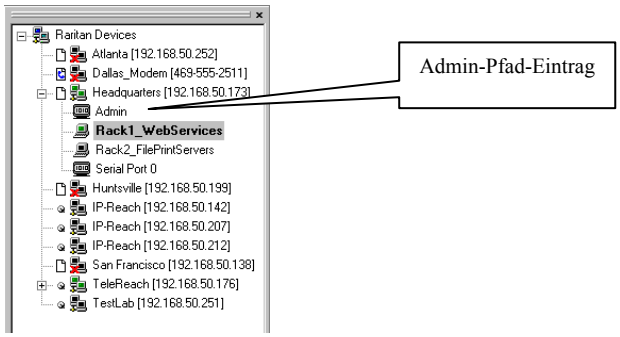
Remoteverwaltung

Alternativ können Sie unter Verwendung von Raritan Remote Client auch remote auf die Verwaltungsfunktionen von IP-Reach zugreifen.

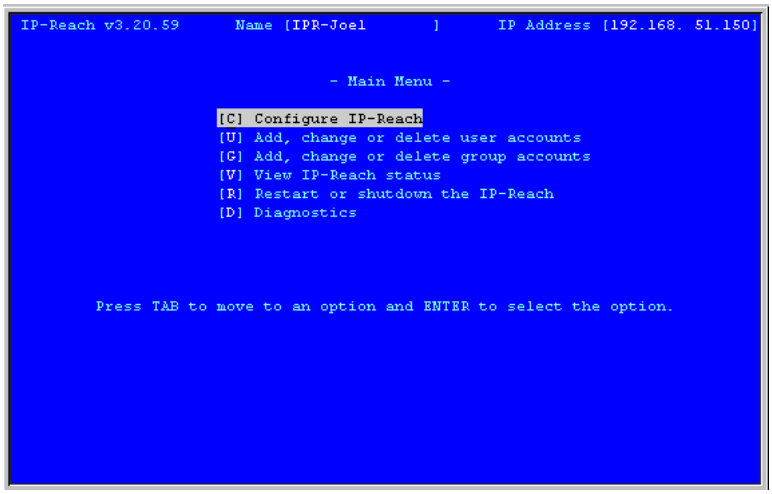
Jeder Administratorbenutzer, der bei IP-Reach über einen Remote-PC angemeldet ist, kann Verwaltungsfunktionen remote ausführen und Änderungen am System vornehmen, sofern IP-Reach für das Zulassen von Remoteadministratorrechten eingerichtet ist (siehe **Allow Remote Administration** [Remoteverwaltung zulassen] im Fenster **Security Configuration** [Sicherheitskonfiguration]).

Hinweis: *Nur Benutzer mit Administratorrechten können auf die Remoteverwaltungsfunktion zugreifen.*

Für den Zugriff auf die Verwaltungsmenüs von Raritan Remote Client doppelklicken Sie auf den Admin-Pfadeintrag, der im RRC-Navigator für die zu konfigurierende IP-Reach-Einheit angezeigt wird.



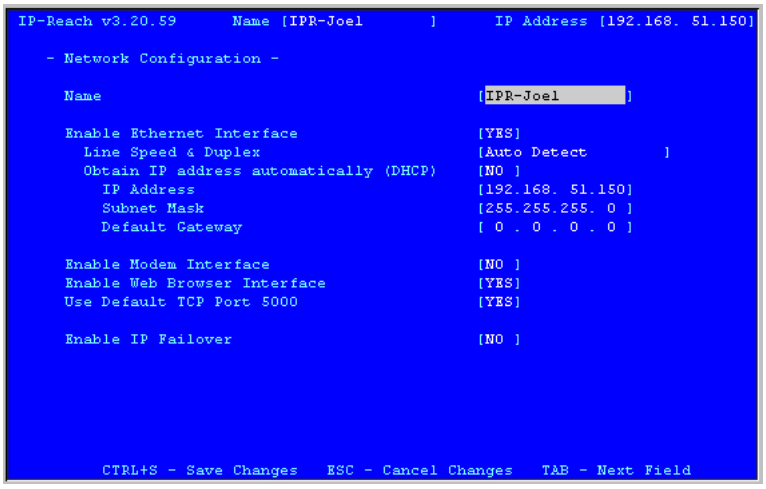
Navigieren in den Verwaltungsmenüs


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Main Menu -
[C] Configure IP-Reach
[U] Add, change or delete user accounts
[G] Add, change or delete group accounts
[V] View IP-Reach status
[R] Restart or shutdown the IP-Reach
[D] Diagnostics
Press TAB to move to an option and ENTER to select the option.

- Verwenden Sie zum Markieren der Auswahl **Configure IP-Reach** (IP-Reach konfigurieren) die Taste <**Tab**>, <↑>, <↓> oder <**C**>, und drücken Sie anschließend die EINGABETASTE. Unter Umständen ist ein Neustart erforderlich.
- Drücken Sie zum Speichern der Änderungen <**Strg+S**>.
- Verwenden Sie zum Markieren der Auswahl **Network Configuration** (Network Configuration) die Taste <**Tab**>, <↑>, <↓> oder <**N**>, und drücken Sie anschließend die EINGABETASTE.

Netzwerkkonfiguration

Drücken Sie nach dem Ändern der Netzwerkkonfiguration zum Speichern auf <**Strg+S**>. Starten Sie den Computer neu, damit alle Änderungen wirksam werden.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Network Configuration -
Name [IPR-Joel]
Enable Ethernet Interface [YES]
Line Speed & Duplex [Auto Detect]
Obtain IP address automatically (DHCP) [NO]
IP Address [192.168. 51.150]
Subnet Mask [255.255.255. 0]
Default Gateway [0 . 0 . 0 . 0]
Enable Modem Interface [NO]
Enable Web Browser Interface [YES]
Use Default TCP Port 5000 [YES]
Enable IP Failover [NO]
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

- **Name:** Vergeben Sie einen eindeutigen Namen für diese IP-Reach-Einheit, zum Beispiel „Hamburger Rechenzentrum“. Der Standardname lautet **IP-Reach**.
- **Enable Ethernet Interface** (Ethernet-Schnittstelle aktivieren)**:** Gibt an, ob IP-Reach seinen Ethernet-Adapter als aktiv zulasssen soll (Standardeinstellung: YES).

Hinweis: *Bei den Netzwerkverbindungen muss es sich um 10BASE-T oder 100BASE-TX Ethernet handeln.*

  - **Line Speed & Duplex** (Übertragungsrate und Duplex)**:** Auto detect 10 Mbps/Full Duplex (Automatische Erkennung 10 MBit/s/Vollduplex), 10 Mbps/Half Duplex (10 MBit/s/Halbduplex), 100 Mbps/Full Duplex (100 MBit/s/Vollduplex) oder 100 Mbps/Half Duplex (100 MBit/s/Halbduplex).
  - **Obtain IP address automatically (DHCP)** (IP-Adresse automatisch zuweisen [DHCP])**:**
    - **YES** (Ja)**:** Aktiviert dynamische IP-Adressen für IP-Reach. Bei jedem Starten von IP-Reach wird eine IP-Adresse vom lokalen DHCP-Server angefordert. Diese Einstellung kann den Remotezugriff auf IP-Reach von außerhalb des LANs erschweren, da die dynamisch zugewiesene IP-Adresse bekannt sein muss, um eine Verbindung zu initiieren.
    - **NO** (Nein)**, Standardeinstellung:** Weist der IP-Reach-Einheit eine feste IP-Adresse zu (empfohlen).
      - **IP Address** (IP-Adresse)**:** Geben Sie die von Ihrem Netzwerkadministrator vergebene IP-Adresse für IP-Reach ein.
      - **Subnet Mask** (Subnetzmaske)**:** Geben Sie eine Subnetzmaske ein. Diese erhalten Sie von Ihrem Netzwerkadministrator.
      - **Default Gateway** (Standardgateway)**:** Geben Sie das Standardgateway ein, sofern Ihr Netzwerkadministrator ein Gateway benennt.
- **Enable Modem Interface** (Modemschnittstelle aktivieren)**:** Aktiviert den Zugriff auf das DFÜ-Modem (Standardeinstellung: YES). Bei IP-Reach-Modellen der M-Serie muss ein externes serielles Modem angeschlossen sein, damit diese Funktion ordnungsgemäß funktioniert (siehe **Kapitel 2: Installation,** ***Physische Anschlüsse der M-Serie, Dedizierter Modemport***).
- **Enable Web Browser Interface** (Webbrowserschnittstelle aktivieren)**:** Aktiviert den Webbrowserzugriff auf IP-Reach (Standardeinstellung: YES).
- **Use Default TCP Port 5000** (Standard-TCP-Port 5000 verwenden)**:**
  - **YES** (Ja)**, Standardeinstellung:** Verwendet den Standardport 5000.
  - **NO** (Nein)**:** Geben Sie eine alternative Portnummer ein.

Hinweis: *Wenn Sie über eine Firewall auf IP-Reach zugreifen möchten, müssen die Firewalleinstellungen die ein- und ausgehende Kommunikation über den Standardport 5000 bzw. den nicht standardmäßigen konfigurierten Port zulassen.*

- **Enable IP Failover** (IP-Ausfallsicherung aktivieren) (nur TR-Serie)**:** Durch diese Einstellung, die nur für Modelle der TR-Serie angezeigt wird, wird der sekundäre Ethernet-Port für die Ausfallsicherung aktiviert.
    - Ist sie aktiviert, prüft IP-Reach die Verfügbarkeit des primären Ethernet-Ports in regelmäßigen Abständen. Der Intervall wird in der Einstellung **Ping Interval in seconds** (Pingintervall in Sekunden) festgelegt.
    - Wenn der primäre Ethernet-Port bei jeder regelmäßigen Pingüberprüfung für einen längeren Intervall nicht verfügbar ist, als in der Einstellung **Failover Timeout in seconds** (Ausfallsicherungszeitlimit in Sekunden) angegeben, deaktiviert IP-Reach seinen primären Ethernet-Port automatisch und aktiviert den sekundären Ethernet-Port.

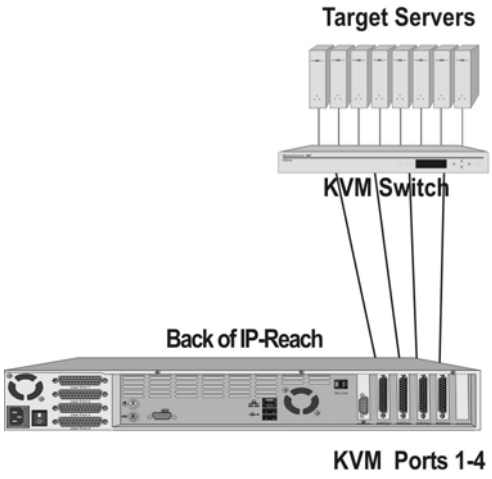
Path Configuration (Pfadkonfiguration)

Wählen Sie im Hauptmenü **Configuration → Path Configuration** (Konfiguration → Pfadkonfiguration), um jeden KVM-Eingangsport zu benennen und IP-Reach-Modelle mit mehreren Ports anzuweisen, neue Sitzungen basierend auf Ihrer Konfiguration auf intelligente Weise umzuleiten. Wenn beispielsweise alle KVM-Eingangsports eines Mehr-Port-IP-Reach-Modells mit demselben Mehrbenutzer-KVM-Switch verbunden sind, kann IP-Reach eingehende Sitzung automatisch zu einem der nicht belegten KVM-Ports umleiten, da sie letztendlich alle mit demselben KVM-Switch verbunden sind.

Den entsprechenden Wert für die Pfadkonfiguration für Ihr Setup können Sie den folgenden Abbildungen entnehmen.

One Path to All Ports (Ein Pfad für alle Ports)**:**

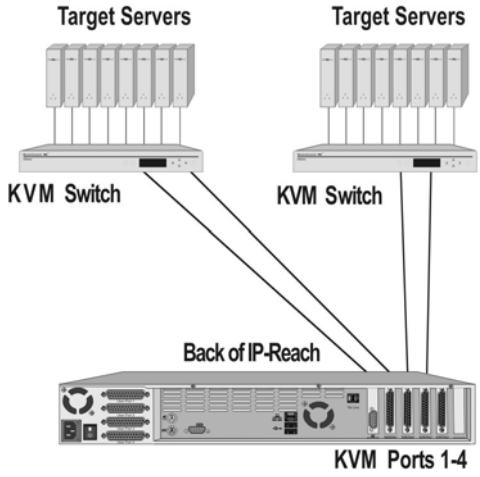
Diese Einstellung wird verwendet, wenn ALLE IP-Reach-KVM-Ports mit nur einer KVM-Switchkonfiguration verbunden sind. Es ist ein Hauptpfad für eine KVM-Konfiguration vorhanden, und bis zu vier Benutzer können eine Verbindung zur KVM-Konfiguration herstellen. IP-Reach weist jedem Benutzer automatisch den nächsten freien Channel des Pfads zu.



***One Path to All Ports** (Ein Pfad für alle Ports)*

Two Paths – Two Ports Each (Zwei Pfade – Jeweils zwei Ports)**:**

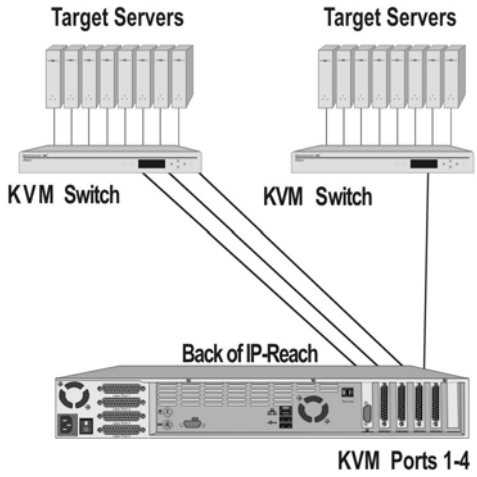
Diese Einstellung wird verwendet, wenn IP-Reach mit zwei KVM-Switchkonfigurationen verbunden ist. Es sind zwei Hauptpfade vorhanden, und zwar einer für jede KVM-Konfiguration. Beim Anmelden bei IP-Reach müssen die Benutzer den Pfad (oder die KVM-Konfiguration) wählen, auf die sie zugreifen möchten. Mit jeder KVM-Konfiguration können maximal zwei Benutzer verbunden sein. IP-Reach weist jedem Benutzer automatisch den nächsten freien Channel des ausgewählten Pfads zu.



Two Paths, Two Ports Each *(Zwei Pfade – Jeweils zwei Ports)*

Two Paths – Three Ports, One Port (3,1) (Zwei Pfade – Drei Ports, ein Port [3,1])**:**

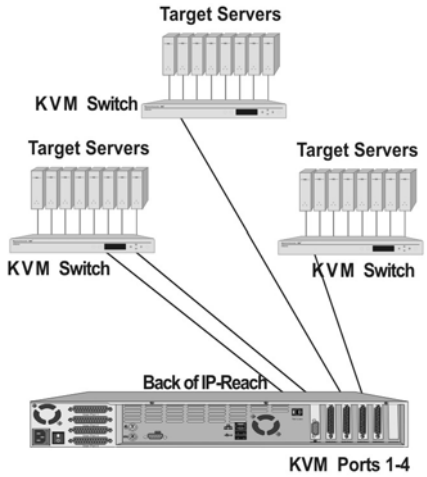
Beim Anmelden bei IP-Reach müssen die Benutzer den Pfad (oder die KVM-Konfiguration, wählen, auf die sie zugreifen möchten. Mit dem ersten Pfad (KVM-Konfiguration) können maximal drei Benutzer verbunden sein. IP-Reach weist jedem Benutzer automatisch den nächsten freien Channel des ausgewählten Pfads zu. Mit dem zweiten Pfad (KVM-Konfiguration) kann nur ein Benutzer verbunden sein.



Two Paths, Three Ports and One Port *(Zwei Pfade, drei Ports und ein Port)*

Three Paths – Two Ports, One Port, One Port (+2, 1, 1) (Drei Pfade – Zwei Ports, ein Port, ein Port [2, 1, 1])**:**

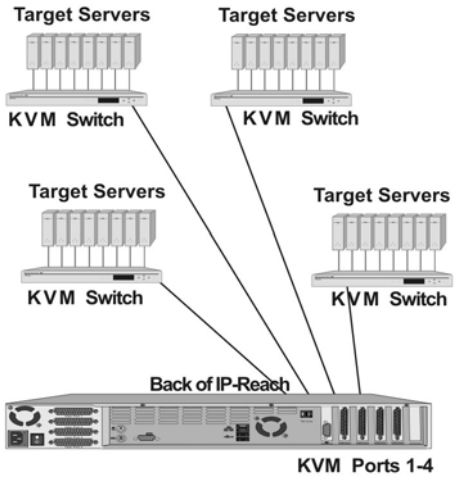
Diese Einstellung wird verwendet, wenn IP-Reach mit drei KVM-Switchkonfigurationen verbunden ist. Es sind drei Hauptpfade vorhanden, und zwar einer für jede KVM-Konfiguration. Beim Anmelden bei IP-Reach müssen die Benutzer den Pfad (oder die KVM-Konfiguration, wählen, auf die sie zugreifen möchten. Mit dem ersten Pfad (KVM-Konfiguration) können maximal zwei Benutzer verbunden sein. IP-Reach weist jedem Benutzer automatisch den nächsten freien Channel des ausgewählten Pfads zu. Mit den übrigen Pfaden (KVM-Konfigurationen) kann jeweils nur ein Benutzer verbunden sein.



Three Paths, Two Ports, One Port, and One Port *(Drei Pfade – Zwei Ports, ein Port, ein Port)*

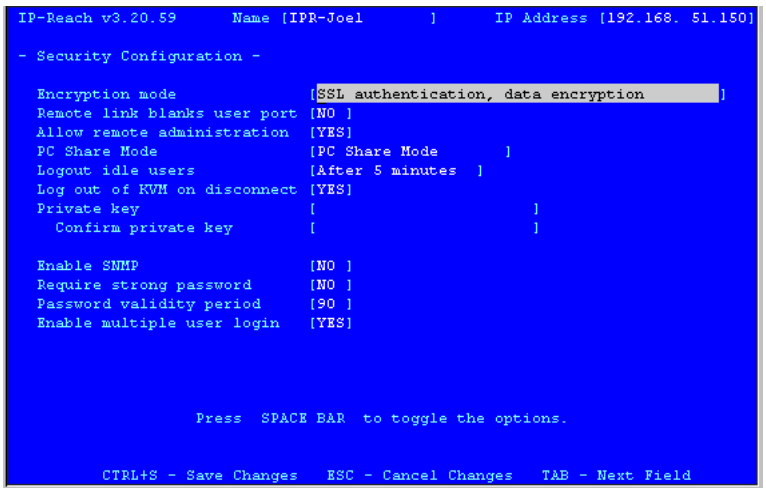
Four Paths (Vier Pfade)**:**

Diese Einstellung wird verwendet, wenn IP-Reach mit vier KVM-Konfigurationen oder vier einzelnen Servern verbunden ist. Es sind vier Hauptpfade vorhanden, und zwar einer für jede KVM-Konfiguration bzw. jeden Server. Beim Anmelden bei IP-Reach müssen die Benutzer den Pfad (oder die KVM-Konfiguration, wählen, auf die sie zugreifen möchten. Mit jedem Pfad (KVM-Konfiguration) kann nur ein Benutzer verbunden sein.



Four Paths *(Vier Pfade)* ***– Ein Port für jeden Pfad***

Sicherheitskonfiguration


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Security Configuration -
Encryption mode [SSL authentication, data encryption]
Remote link blanks user port [NO]
Allow remote administration [YES]
PC Share Mode [PC Share Mode]
Logout idle users [After 5 minutes]
Log out of KVM on disconnect [YES]
Private key [ ]
Confirm private key [ ]
Enable SNMP [NO]
Require strong password [NO]
Password validity period [90]
Enable multiple user login [YES]
Press SPACE BAR to toggle the options.
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

- **Encryption mode** (Verschlüsselungsmodus): Wählen Sie aus den vorhandenen Optionen die gewünschte Verschlüsselungsebene für die Anfangsverbindungsauthentifizierung und die Videodatenübertragung der Remotesitzung aus.
  - **No encryption** (Keine Verschlüsselung)**:** Keine Verschlüsselung oder Sicherheit. Weder die Anfangsverbindungsauthentifizierung noch die Remotevideodatenübertragung wird verschlüsselt.
  - **SSL authentication, NO data encryption** (SSL-Authentifizierung, KEINE Datenverschlüsselung)**:** In diesem Modus werden Benutzernamen und Kennwörter gesichert, jedoch keine KVM-Daten. Das 128-Bit-SSL-Protokoll (Secure Socket Layer) stellt während der Anfangsverbindungsauthentifizierung einen privaten Kommunikationschannel zwischen IP-Reach und dem Remote-PC bereit. Während der Remote-KVM-Datenübertragung findet keine Verschlüsselung statt.
  - **SSL authentication, data encryption** (SSL-Authentifizierung, Datenverschlüsselung)**, Standardeinstellung:** In diesem Modus werden Benutzernamen, Kennwörter und KVM-Daten gesichert. Das 128-Bit-SSL-Protokoll (Secure Socket Layer) stellt während der Anfangsverbindungsauthentifizierung einen privaten Kommunikationschannel zwischen IP-Reach und dem Remote-PC bereit. Nach der Authentifizierung werden die KVM-Daten ebenfalls mit der 128-Bit-Verschlüsselung übertragen, es wird jedoch ein anbietereigenes Protokoll verwendet, das effizienter ist als SSL.
  - **SSL authentication, SSL data encryption** (SSL-Authentifizierung, SSL-Datenverschlüsselung)**:** Dieser Modus sichert Benutzernamen und Kennwörter und bietet eine hohe Sicherheit für KVM-Daten. Das 128-Bit-SSL-Protokoll (Secure Socket Layer) stellt während der Anfangsverbindungsauthentifizierung einen privaten Kommunikationschannel zwischen IP-Reach und dem Remote-PC bereit. Während der Remote-KVM-Datenübertragung findet ebenfalls eine 128-Bit-SSL-Verschlüsselung statt.

Hinweis: *Durch die SSL-Datenverschlüsselung wird die über die Remoteverbindung zu übertragene Datenmenge erhöht. Daher wird sie für Modem- oder sehr langsame Internetverbindungen nicht empfohlen. Die Standardeinstellung* ***SSL authentication, data encryption*** *(SSL-Authentifizierung, Datenverschlüsselung) bietet die gleiche Sicherheitsebene bei höherer Effizienz.*

- **Remote link blanks user port** (Remoteverbindung deaktiviert den Benutzerport)**:** Bestimmt, ob ein direkter analoger Benutzerport lokal deaktiviert wird, sobald ein Remotebenutzer auf den entsprechenden KVM-Port zugreift. So bleiben dem lokalen Benutzer die Aktivitäten des Remotebenutzers verborgen.
  - **NO** (Nein)**, Standardeinstellung:** Der Benutzerport kann lokal angezeigt werden, während der Remotebenutzer darauf zugreift.
  - **YES** (Ja)**:** Der Benutzerport kann nicht lokal angezeigt werden, während der Remotebenutzer darauf zugreift. Die lokale oder direkte analoge Benutzerkonsole unterbricht die Videoanzeige.

Hinweis: *Benutzerkonsolen können an die Benutzerports 1 bis 4 angeschlossen werden. Jede Benutzerkonsole zeigt den Pfad des entsprechenden KVM-Ports an. Die mit Benutzerport 1 verbundene Benutzerkonsole zeigt beispielsweise den mit KVM-Port 1 verbundenen KVM-Pfad an. Ebenso zeigt die mit Benutzerport 2 verbundene Benutzerkonsole den mit KVM-Port 2 verbundenen KVM-Pfad an usw.*

- **Allow remote administration** (Remoteverwaltung zulassen)**:**
  - **NO** (Nein)**:** Mit dieser Einstellung ist der Zugriff auf alle Verwaltungsfunktionen nur von der IP-Reach-Verwaltungskonsole, nicht aber von einem Remote-PC verfügbar.
  - **YES** (Ja)**, Standardeinstellung:** Ermöglicht Remotezugriff auf alle Verwaltungsfunktionen von IP-Reach für Administratoren, die bei einem Remote-PC angemeldet sind. Weitere Informationen finden Sie in **Kapitel 3: Raritan Remote Client, Remotegeräteadministration.**
- **PC Share Mode** (PC-Freigabemodus)**:** Bestimmt den globalen gleichzeitigen Remotezugriff. Ermöglicht bis zu acht Remotebenutzern die gleichzeitige Anmeldung an einer IP-Reach-Einheit sowie die gleichzeitige Anzeige und Steuerung eines Zielservers über IP-Reach. Da die Steuerung auf der ersten aktiven Tastatur-/Mauseingabe basiert, ist u.U. eine ungleichmäßige Steuerung festzustellen, wenn mehrere Remotebenutzer genau zum gleichem Zeitpunkt Tastatureingaben vornehmen oder die Maus bewegen.
  - **Private Mode** (Privater Modus)**, Standardeinstellung:** PCs werden nicht freigegeben. Auf jeden IP-Reach-Pfad kann nur ein Benutzer zurzeit zugreifen.
  - **PC Share Mode** (PC-Freigabemodus)**:** Auf IP-Reach kann mehr als ein Benutzer (mit oder ohne Administratorberechtigung) zurzeit zugreifen. Da die Steuerung auf der ersten aktiven Tastatur-/Mauseingabe basiert, ist u.U. eine ungleichmäßige Steuerung festzustellen, wenn mehrere Remotebenutzer genau zum gleichem Zeitpunkt Tastatureingaben vornehmen oder die Maus bewegen.
  - **PC Share Admins Only** (PC-Freigabe nur für Administratoren)**:** Auf IP-Reach kann mehr als ein Benutzer (nur Administratoren) zurzeit zugreifen. Da die Steuerung auf der ersten aktiven Tastatur-/Mauseingabe basiert, ist u.U. eine ungleichmäßige Steuerung festzustellen, wenn mehrere Remotebenutzer genau zum gleichem Zeitpunkt Tastatureingaben vornehmen oder die Maus bewegen.

Hinweis: *Der PC-Freigabemodus ist eine globale Einstellung. Zugriffseinstellungen für einzelne Benutzer können im Fenster* ***User Account Settings*** *(Benutzerkonteneinstellungen) unter* ***Keyboard and Mouse Control*** *(Tastatur- und Maussteuerung) und* ***Concurrent Access Mode*** *(Gleichzeitiger Zugriffsmodus) vorgenommen werden. In jedem Benutzerprofil können die Tastatur- und Maussteuerung sowie der gleichzeitige Zugriff einzeln aktiviert/deaktiviert werden.*

- **Logout idle users** (Inaktive Benutzer abmelden)**:** Bietet eine Option für IP-Reach, die die Verbindung von inaktiven Remotebenutzern nach bestimmten ausgewählten Zeitintervallen trennt.
  - **Never** (Nie)**, Standardeinstellung:** Inaktive Remotebenutzer werden nie getrennt.
  - **After 5, 15, 30, 60, or 120 minutes** (Nach 5, 15, 30, 60 oder 120 Minuten)**:** Inaktive Remotebenutzer werden automatisch von IP-Reach getrennt, nachdem der ausgewählte Zeitraum verstrichen ist, ohne dass eine aktive Eingabe vom Remote-PC erfolgt ist.
- **Log out of KVM on disconnect** (Beim Trennen bei KVM abmelden)**:** Legt die automatische Abmeldung von der OSD des verbundenen KVM fest.
  - **NO** (Nein)**, Standardeinstellung:** Es werden keine speziellen Befehle erteilt für die OSD des verbundenen KVM-Switches bei der Trennung des Remotebenutzers von IP-Reach. Wenn ein Remotebenutzer die Verbindung zu IP-Reach trennt, bleibt die OSD des verbundenen KVM-Switch in dem Zustand, der dem Benutzer zuletzt angezeigt wurde.
  - **YES** (Ja)**:** Trennt ein Remotebenutzer die Verbindung zu IP-Reach, sendet IP-Reach automatisch einen Abmeldungsbefehl (**<F9>**) an den verbundenen KVM-Switch.

Hinweis: *Bei gleichzeitigen Verbindungen wird der Abmeldungsbefehl, sofern festgelegt, gesendet, sobald sich der letzte verbundene Benutzer von IP-Reach abmeldet.*

Hinweis: *Damit die Option zur Abmeldung von KVM ordnungsgemäß funktioniert, muss IP-Reach für die Zugriffstaste des grundlegenden KVM-Switches konfiguriert sein (siehe Kapitel 3: Raritan Remote Client, Remotegeräteadministration).*

- **Restrict remote IP address** (Remote-IP-Adresse beschränken)**:** Bestimmt, welchen Remote-IP-Adresssen Zugriff auf IP-Reach gewährt wird.
  - **NO** (Nein)**, Standardeinstellung:** Der Remotezugriff auf IP-Reach ist unbeschränkt.
  - **YES** (Ja)**:** IP-Reach gewährt bis zu vier bezeichneten IP-Adressen oder IP-Adressebenen Zugriff. Administratoren können IP-Reach so einrichten, dass nur Anforderungen vom Intranet des Unternehmens und/oder von einigen externen IP-Adressen akzeptiert werden. Die IP-Maskenfelder bestimmen, welchen Remote-IP-Adressen IP-Reach Remotezugriff gewährt.
    - Eine bestimmte IP-Maske weist IP-Reach an, Remotezugriff nur auf diese bestimmte Remote-IP-Adresse zu gewähren. Die Maske 10.0.0.1 weist IP-Reach beispielsweise an, Remotezugriff nur vom Remote-IP-Adressstandort 10.0.0.1 zu gewähren.

- Der Wert 255 dient bei der Angabe der IP-Maskenadresse als Platzhalter. Die Maske 10.0.0.255 weist IP-Reach beispielsweise an, Remotezugriff nur von einem Remote-IP-Adressstandort im Bereich von 10.0.0.0 bis 10.0.0.255 zu gewähren. Ebenso weist die Maske 192.255.255.255 IP-Reach an, Remotezugriff nur von einem Remote-IP-Adressstandort zu gewähren, der mit 192 beginnt.

Hinweis: *Sobald die* ***Option Restrict remote IP address*** *(Remote-IP-Adresse beschränken) aktiviert wurde, muss in mindestens einem IP-Maskenfeld ein Eintrag vorgenommen werden, da 0.0.0.0 eine ungültige IP-Adresse ist.*

- **Private Key** (Privater Schlüssel)**:** Geben Sie ein privates Schlüsselkennwort ein. Dieser private Schlüssel dient als Kennwortschutz auf zweiter Ebene. Nur Remotebenutzer, denen neben ihrem Benutzernamen und dem Kennwort auch das private Schlüsselkennwort bekannt ist, können sich anmelden und eine Verbindung zu IP-Reach herstellen.
  - **Confirm private key** (Privaten Schlüssel bestätigen)**:** Geben Sie das private Schlüsselkennwort zur Bestätigung erneut ein.

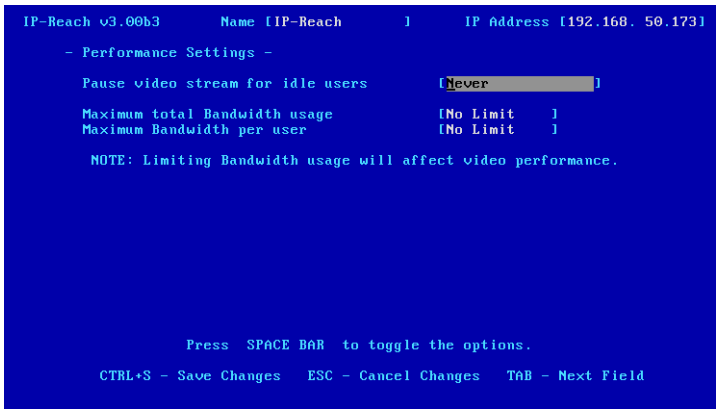
Hinweis: *Private Schlüsselkennwörter unterliegen der Groß-/Kleinschreibung. Für Remotebenutzeranmeldungen müssen Kennwörter genau in der hier erstellten Kombination von Groß-/Kleinbuchstaben eingegeben werden.*

Hinweis: *Private Schlüsselkennwörter müssen aus alphanumerischen Zeichen bestehen. Sonderzeichen sind nicht erlaubt.*

- **Enable SNMP** (SNMP aktivieren)**:** Bestimmt, ob IP-Reach auf SNMP GET REQUESTS antwortet oder nicht.
- **Require strong password** (Sicheres Kennwort erfordern)**:** Erfordert für Benutzerkennwörter eine Mindestlänge von 6 Zeichen sowie mindestens ein alphabetisches Zeichen und ein nicht-alphabetisches Zeichen (Satzzeichen oder Ziffer). Die ersten vier Zeichen des Kennworts und des Benutzernamens dürfen nicht identisch sein.
- **Password validity period** (Kennwortgültigkeitsdauer)**:** Geben Sie eine Anzahl von Tagen in dieses Feld ein, um festzulegen, dass die Benutzer ihre Kennwörter nach einem definierten Zeitraum ändern müssen.
- **Enable multiple user login** (Mehrere Benutzeranmeldungen aktivieren)**:** Bei Auswahl dieser Regel kann eine Benutzername-/Kennwortkombination von mehreren Clientworkstations gleichzeitig verwendet werden, um eine Verbindung mit IP-Reach herzustellen.

Leistungseinstellungen

Im Fenster **Performance Settings** (Leistungseinstellungen) werden die IP-Reach-Parameter für die Videodatenübertragung und die Bandbreite eingerichtet.


IP-Reach v3.00b3 Name [IP-Reach] IP Address [192.168. 50.173]
- Performance Settings -
Pause video stream for idle users [Never]
Maximum total Bandwidth usage [No Limit]
Maximum Bandwidth per user [No Limit]
NOTE: Limiting Bandwidth usage will affect video performance.
Press SPACE BAR to toggle the options.
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

- **Pause video stream for idle users** (Videodatenstrom für inaktive Benutzer unterbrechen)**:** Durch Unterbrechen des Videodatenstroms bei anhaltender Inaktivität wird verhindert, dass inaktive Benutzer unnötig Bandbreite verbrauchen.
  - **Never** (Nie)**, Standardeinstellung:** Videodaten werden ständig an den Remote-PC gesendet und das Fenster permanent aktualisiert, auch wenn der Remotebenutzer inaktiv ist und keine aktiven Eingaben an IP-Reach sendet.

- **After 5, 15, 30, 60, or 120 minutes** (Nach 5, 15, 30, 60 oder 120 Minuten)**:** Der Videodatenstrom zum Remote-PC wird unterbrochen, nachdem der ausgewählte Zeitraum verstrichen ist, ohne dass eine aktive Eingabe vom Remote-PC erfolgt ist.

- **Maximum total Bandwidth usage** (Gesamte maximale Bandbreitennutzung)**:** Legt eine Höchstgrenze für die Bandbreite fest, die von dieser IP-Reach-Einheit genutzt werden darf.
  - **No Limit** (Kein Beschränkung)**, Standardeinstellung:** IP-Reach kann so viel Bandbreite nutzen, wie erforderlich.
  - **10, 5, 2 oder 1 MB oder 512, 256, 128 KB:** Die gesamte Bandbreite, die dieser IP-Reach-**Einheit** zur Verfügung steht, ist auf den ausgewählten Wert beschränkt. Je geringer die zulässige Bandbreite ist, desto langsamer kann die resultierende Leistung sein.
- **Maximum Bandwidth per user** (Maximale Bandbreite pro Benutzer)**:** Legt eine Höchstgrenze für die Bandbreite fest, die von den einzelnen an dieser IP-Reach-Einheit angemeldeten Benutzern genutzt werden darf.

Hinweis: *Die Verfügbarkeit von gleichzeitigem Remotezugriff wird durch die globale Einstellung* ***PC Share Mode*** *(PC-Freigabemodus) im Fenster* ***Security Configuration*** *(Sicherheitskonfiguration) oder individuell durch jedes Benutzerprofil über die Option* ***Keyboard and Mouse Control*** *(Tastatur- und Maussteuerung) und* ***Concurrent Access Mode*** *(Gleichzeitiger Zugriffsmodus) im Fenster* ***User Account Settings*** *(Benutzerkonteneinstellugnen) bestimmt. Da die Steuerung von IP-Reach und einem verbundenen Zielserver auf der ersten aktiven Tastatur-/Mauseingabe basiert, ist u.U. eine ungleichmäßige Steuerung festzustellen, wenn mehrere Remotebenutzer genau zum gleichen Zeitpunkt Tastatureingaben vornehmen oder die Maus bewegen.*

  - **No Limit** (Kein Beschränkung)**, Standardeinstellung:** Jeder **aktive** Benutzer kann so viel Bandbreite nutzen, wie erforderlich.
  - **10, 5, 2 oder 1 MB oder 512, 256, 128 KB:** Die von jedem aktiven Benutzer während des Betriebs dieser IP-Reach-Einheit genutzte Bandbreite ist auf den ausgewählten Wert beschränkt. Je geringer die zulässige Bandbreite ist, desto langsamer kann die resultierende Leistung sein.

Drücken Sie <**Strg+S**> zum Speichern der Änderungen oder <**Esc**>, um die Änderungen abzubrechen, und kehren Sie zum Konfigurationsmenü zurück. Gespeicherte Änderungen der Leistungseinstellungen werden erst wirksam, wenn IP-Reach neu gestartet wird.

Wichtig: Die Ausführungen der nächsten beiden Abschnitte *Remoteauthentifizierung: Benutzer, Gruppen und Zugriffsberechtigungen* und *Implementierung der Remoteauthentifizierung* unterscheiden sich erheblich von Version 3.1. Lesen Sie diese Abschnitte sorgfältig durch.

Remoteauthentifizierung: Benutzer, Gruppen und Zugriffsberechtigungen

Überblick

IP-Reach verwaltet eine interne Liste von Benutzer- und Gruppennamen, um die Zugriffsautorisierung und die Berechtigungen festzulegen. Diese Informationen werden intern in einem verschlüsselten Format gespeichert.

Hinweis für CommandCenter-Benutzer

Wenn Sie IP-Reach in die Verwaltungsanwendung CommandCenter von Raritan integrieren und damit steuern möchten, gilt dieser Abschnitt des Benutzerhandbuchs nicht für Sie. Wenn eine IP-Reach-Einheit über CommandCenter gesteuert wird, bestimmt CommandCenter die zulässigen Benutzer und Gruppen. Weitere Informationen finden Sie im CommandCenter-Benutzerhandbuch.

Hinweis für Raritan-Kunden, die vorhergehende Firmwareversionen aktualisieren

Wenn Sie zuvor bereits Raritan-Produkte wie den Dominion KSX und IP-Reach mit älteren Firmwareversionen als Version 3.2 konfiguriert haben, sollten Sie diesen Abschnitt sorgfältig lesen. Beginnend mit Firmwareversion 3.2 wurde die Implementierung von Benutzern und Gruppen erheblich geändert, um flexiblere und leistungsstärkere Konfigurationen zu ermöglichen.

Beziehung zwischen Benutzern und Gruppeneinträgen

IP-Reach weist allen Benutzern eine Gruppe zu. Die Zuweisung von Benutzern zu Gruppen ermöglicht die gleichzeitige Verwaltung von Berechtigungen für alle Benutzer in einer bestimmten Gruppe. Auf diese Weise müssen die Berechtigungen nicht für jeden Benutzer einzeln verwaltet werden.

- **Benutzerinformationen** dienen zur Benutzerauthentifizierung (d.h., ist ein bestimmter Benutzer überhaupt berechtigt, auf IP-Reach zuzugreifen?).
- **Gruppeninformationen** dienen zur Authentifizierung aller Benutzer einer bestimmten Gruppe (d.h., für welche Ports des IP-Reach-Geräts besitzen die Benutzer in einer Gruppe Zugriffsberechtigung?).

Sie können bei Bedarf darauf verzichten, spezifische Benutzer Gruppen zuzuordnen. In diesem Fall klassifiziert IP-Reach den jeweiligen Benutzer als „Einzelperson“.

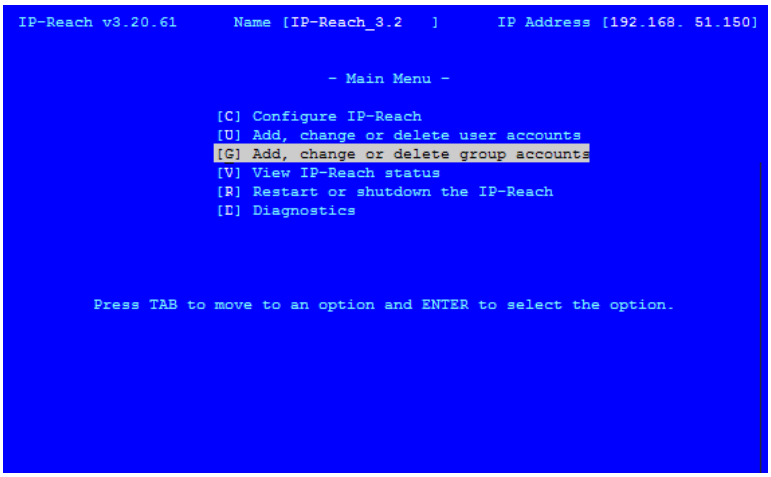
Erforderliche Benutzergruppen

Jedes IP-Reach-Gerät enthält drei Standardbenutzergruppen. Diese Gruppen können nicht gelöscht werden:

ADMIN	Benutzergruppe für den ursprünglichen vordefinierten administrativen Benutzer.
NONE (KEINE)	Für diese Gruppe definierte Berechtigungen werden für einen Benutzer verwendet, wenn IP-Reach für die Remoteauthentifizierung über LDAP oder RADIUS konfiguriert ist (siehe hierzu den nächsten Abschnitt) und ein Anmeldeversuch erfolgreich ist, vom Remoteauthentifizierungsserver jedoch keine Benutzergruppe zurückgegeben wird.
UNKNOWN (UNBEKANNT)	Für diese Gruppe definierte Berechtigungen werden für einen Benutzer verwendet, wenn IP-Reach für die Remoteauthentifizierung über LDAP oder RADIUS konfiguriert ist (siehe hierzu den nächsten Abschnitt) und ein Anmeldeversuch erfolgreich ist, die vom Remoteauthentifizierungsserver zurückgegebene Benutzergruppe jedoch nicht in IP-Reach gefunden wird.

Erstellen oder Ändern von Gruppenkonten

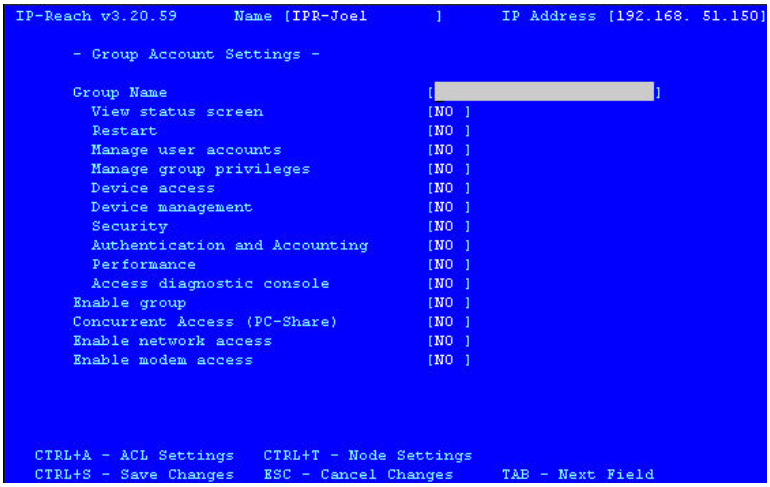
1. Geben Sie zum Hinzufügen oder Ändern eines Gruppenkontos im Hauptmenü <**G**> ein.


IP-Reach v3.20.61 Name [IP-Reach_3.2] IP Address [192.168. 51.150]
- Main Menu -
[C] Configure IP-Reach
[U] Add, change or delete user accounts
[G] Add, change or delete group accounts
[V] View IP-Reach status
[R] Restart or shutdown the IP-Reach
[D] Diagnostics
Press TAB to move to an option and ENTER to select the option.

2. Das Fenster **Group Account** (Gruppenkonto) wird geöffnet.
   a. Geben Sie den Buchstaben **<A>** ein, um ein neues Gruppenkonto hinzuzufügen.
   b. Verwenden Sie beim Ändern der Gruppenkontoeigenschaften die **<TAB>**-Taste, um sich durch die Liste zu bewegen, und drücken Sie die EINGABETASTE, um eine zu ändernde Gruppe auszuwählen.

IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
Group Account
ADMIN
A - Add a new group TAB - Next Group C - Change Group D - Delete group
ESC - Exit N - Next page P - Previous page

3. Das Fenster **Group Account Settings** (Gruppenkontoeinstellungen) wird geöffnet.
   a. Geben Sie den Gruppenkontonamen in das Feld **Group Name** (Gruppenname) ein. Der Name kann alphanumerische Zeichen enthalten und maximal 24 Zeichen umfassen, wobei das erste Zeichen keine Zahl sein darf.
   b. Bewegen Sie sich anhand der Pfeiltasten <↑> und <↓> oder der <**TAB**>-Taste durch die Zeilenelemente und drücken Sie die LEERTASTE, um zwischen **YES** (JA) und **NO** (NEIN) zu wechseln. Drücken Sie nach abgeschlossener Bearbeitung auf <**STRG**> + <**S**>, um Ihre Daten zu speichern, oder auf <**ESC**>, um das Fenster ohne Speichern der Eingaben zu beenden.

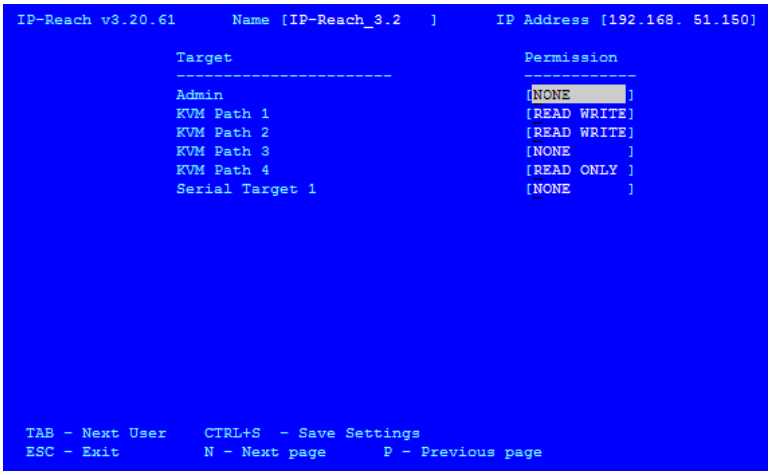

IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Group Account Settings -
Group Name
View status screen [NO]
Restart [NO]
Manage user accounts [NO]
Manage group privileges [NO]
Device access [NO]
Device management [NO]
Security [NO]
Authentication and Accounting [NO]
Performance [NO]
Access diagnostic console [NO]
Enable group [NO]
Concurrent Access (PC-Share) [NO]
Enable network access [NO]
Enable modem access [NO]
CTRL+A - ACL Settings CTRL+T - Node Settings
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

4. Drücken Sie zum Speichern der Änderungen auf <**STRG**> + <**S**>.

Zuweisen von Portzugriffsberechtigungen

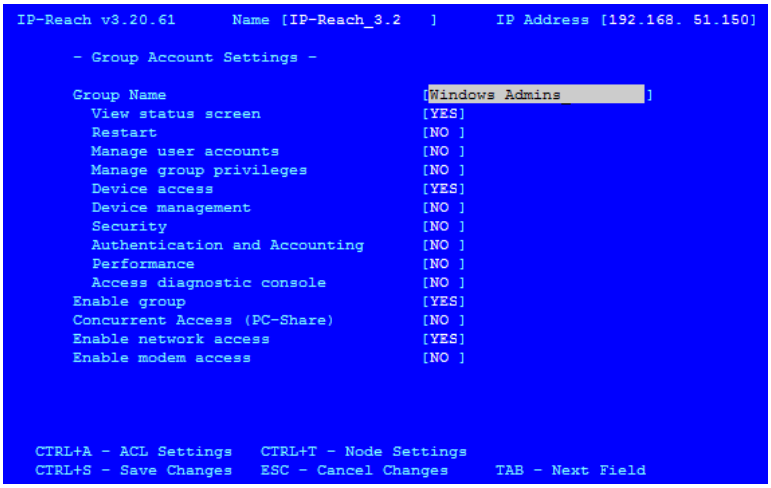
Standardmäßig verfügen alle neuen Benutzergruppen nicht über Zugriffsberechtigung auf einen KVM- oder seriellen Port von IP-Reach. Jeder Benutzergruppe müssen Zugriffsberechtigungen erst zugewiesen werden.

1. Drücken Sie beim Erstellen einer Gruppe oder Bearbeiten einer vorhandenen Gruppe im Fenster **Group Account Settings** (Gruppenkontoeinstellungen) auf <**STRG**>+<**T**>, um die Option **Node Settings**. (Knoteneinstellungen) auszuwählen.
2. Das Menü **Node Settings** (Knoteneinstellungen) wird angezeigt. Es führt jeden auf Ihrem IP-Reach konfigurierten KVM- und seriellen Port auf.


IP-Reach v3.20.61 Name [IP-Reach_3.2] IP Address [192.168. 51.150]
Target Permission
Admin [NONE]
KVM Path 1 [READ WRITE]
KVM Path 2 [READ WRITE]
KVM Path 3 [NONE]
KVM Path 4 [READ ONLY]
Serial Target 1 [NONE]
TAB - Next User CTRL+S - Save Settings
ESC - Exit N - Next page P - Previous page

3. Scollen Sie mithilfe der Pfeiltasten <↑> und <↓> durch die einzelnen auf Ihrem IP-Reach konfigurierten KVM- und seriellen Ports und drücken Sie die LEERTASTE, um folgende Optionen zu aktivieren und zu deaktivieren:
   a. **NONE** (KEINE) – Benutzer in dieser Gruppe besitzen keinerlei Zugriffsberechtigung für diesen KVM- oder seriellen Port. Der Port wird für Benutzer dieser Gruppe nicht einmal als Option angezeigt.
   b. **READ ONLY** (NUR LESEZUGRIFF) – Benutzer in dieser Gruppe sind berechtigt, diesen KVM- oder seriellen Konsolenport anzuzeigen, können ihn jedoch nicht steuern (Eingaben vornehmen, die Maus bewegen usw.).
   c. **READ WRITE** (LESE- UND SCHREIBZUGRIFF) – Benutzer in dieser Gruppe besitzen die Berechtigung, diesen KVM- oder seriellen Konsolenport anzuzeigen und können ihn auch steuern.

4. Drücken Sie zum Speichern auf <**STRG**>+<**S**>.
5. Ihre Änderungen sind **noch nicht gespeichert**. Sie kehren zum Fenster **Group Account Settings** (Gruppenkontoeinstellungen) für die Benutzergruppe zurück, die Sie bearbeiten bzw. erstellen.


IP-Reach v3.20.61 Name [IP-Reach_3.2] IP Address [192.168. 51.150]
- Group Account Settings -
Group Name [Windows Admins]
View status screen [YES]
Restart [NO]
Manage user accounts [NO]
Manage group privileges [NO]
Device access [YES]
Device management [NO]
Security [NO]
Authentication and Accounting [NO]
Performance [NO]
Access diagnostic console [NO]
Enable group [YES]
Concurrent Access (PC-Share) [NO]
Enable network access [YES]
Enable modem access [NO]
CTRL+A - ACL Settings CTRL+T - Node Settings
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

6. Drücken Sie in diesem Fenster die Tastenkombination <**STRG**>+<**S**> erneut, um die Berechtigungseinstellungen für die entsprechende Benutzergruppe zu speichern.

Löschen von Gruppenkonten

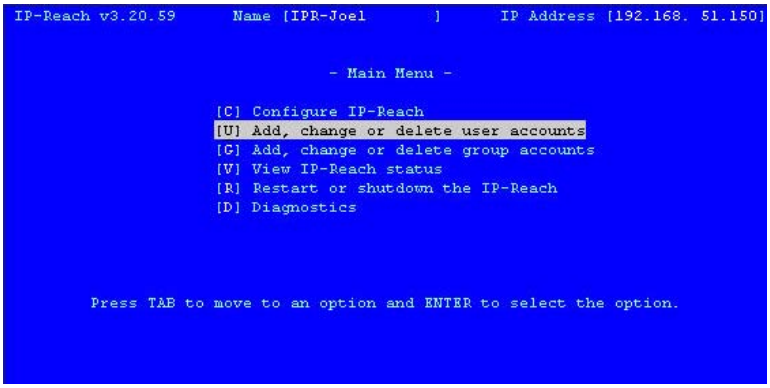
Geben Sie zum Löschen eines vorhandenen Gruppenkontos den Buchstaben <**G**> im Hauptmenü ein. Drücken Sie im Fenster **Group Account** (Gruppenkonto) die <**TAB**>-Taste, um das zu löschende Gruppenkonto auszuwählen, und drücken Sie anschließend die Taste <**D**>. Stellen Sie vor dem Löschen einer Gruppe sicher, dass dieser keine Benutzer zugewiesen sind. Andernfalls werden diese Benutzer gelöscht.

Die Standardgruppe **ADMIN** kann nicht gelöscht werden.

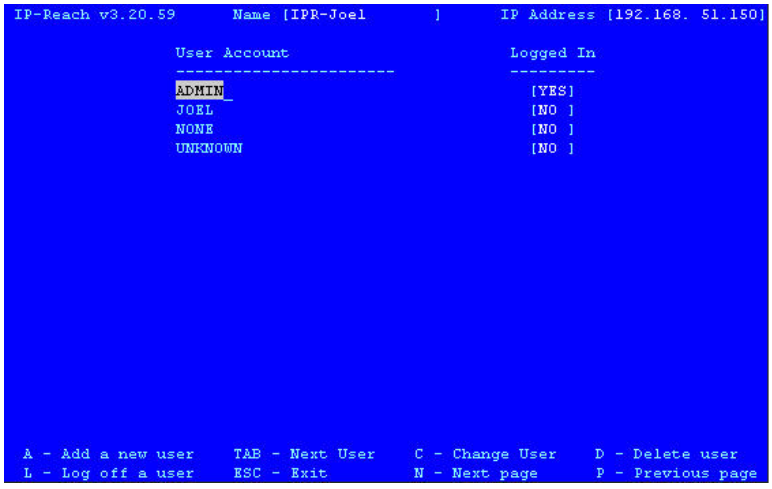
IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
Group Account
ADMIN
A - Add a new group TAB - Next Group C - Change Group D - Delete group
ESC - Exit N - Next page P - Previous page

Erstellen oder Ändern von Benutzerkonten

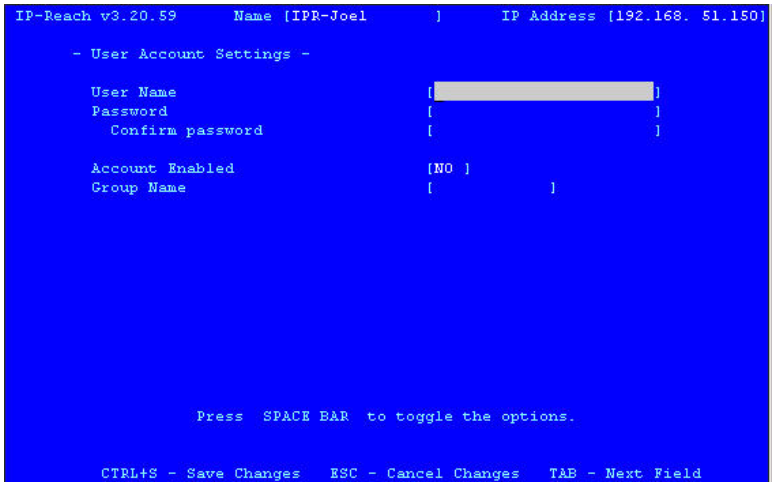
1. Geben Sie zum Hinzufügen oder Ändern eines Benutzerkontos im Hauptmenü <**U**> ein.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Main Menu -
[C] Configure IP-Reach
[U] Add, change or delete user accounts
[G] Add, change or delete group accounts
[V] View IP-Reach status
[R] Restart or shutdown the IP-Reach
[D] Diagnostics
Press TAB to move to an option and ENTER to select the option.

2. Das Fenster **User Account** (Benutzerkonto) wird angezeigt.
   a. Geben Sie den Buchstaben **<A>** ein, um ein neues Benutzerkonto hinzuzufügen.
   b. Verwenden Sie beim Ändern der Benutzerkontoeigenschaften die **<TAB>**-Taste, um sich durch die Liste zu bewegen, und drücken Sie die EINGABETASTE, um einen zu ändernden Benutzer auszuwählen.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
User Account Logged In
ADMIN [YES]
JOEL [NO]
NONE [NO]
UNKNOWN [NO]
A - Add a new user TAB - Next User C - Change User D - Delete user
L - Log off a user ESC - Exit N - Next page P - Previous page

3. Das Fenster **User Account Settings** (Benutzerkontoeinstellungen) wird geöffnet.
   a. Geben Sie den Namen des Benutzers in das Feld **User Name** (Benutzername) ein. Der Name kann alphanumerische Zeichen enthalten und maximal 24 Zeichen umfassen, wobei das erste Zeichen keine Zahl sein darf.
   b. Geben Sie das Kennwort des Benutzers in das Feld **Password** (Kennwort) ein. Das Kennwort kann alphanumerische Zeichen enthalten und insgesamt bis zu 23 Zeichen umfassen.
   c. Geben Sie das Kennwort zur Bestätigung in das Feld **Confirm password** (Kennwort bestätigen) ein.
   d. Drücken Sie im Feld **Account Enabled** (Konto aktiviert) die LEERTASTE, um das Konto des Benutzers durch YES (JA) und NO (NEIN) zu aktivieren bzw. zu deaktivieren (Standardeinstellung: NO).
   e. Geben Sie in das Feld **Group Name** (Gruppenname) den Namen der Gruppe ein, zu der dieser Benutzer gehört.
   f. Drücken Sie nach Abschluss Ihrer Eingaben die Tasten **<STRG>** + **<S>**, um die Daten zu speichern, oder **<ESC>**, um das Fenster ohne Speichern der Daten zu beenden.

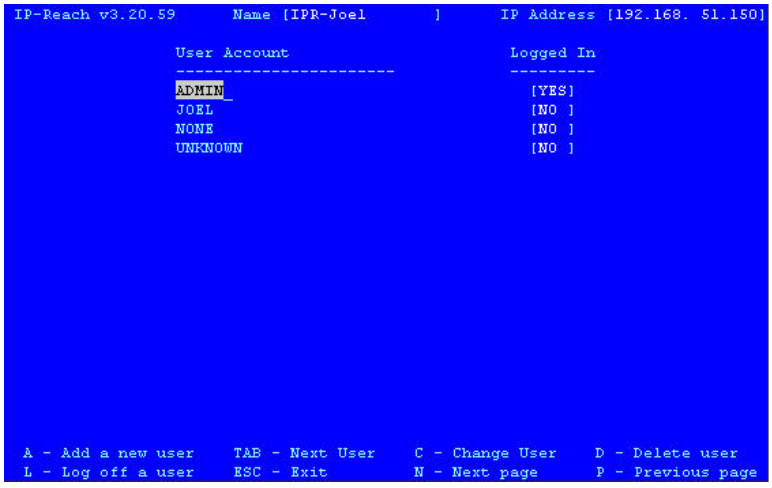

IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- User Account Settings -
User Name
Password
Confirm password
Account Enabled [NO]
Group Name
Press SPACE BAR to toggle the options.
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

4. Drücken Sie <**STRG**> + <**M**>, um zum Hauptmenü zurückzukehren.

Benutzerkonten löschen

Geben Sie zum Löschen eines vorhandenen Benutzerkontos den Buchstaben <**U**> im Hauptmenü ein. Drücken Sie im Fenster **User Account** (Benutzerkonto) die <**TAB**>-Taste, um das zu löschende Benutzerkonto auszuwählen, und drücken Sie anschließend die Taste <**D**>.

Der Standardbenutzer **ADMIN** kann nicht gelöscht werden.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
User Account
Logged In
ADMIN [YES]
JOEL [NO]
NONE [NO]
UNKNOWN [NO]
A - Add a new user TAB - Next User C - Change User D - Delete user
L - Log off a user ESC - Exit N - Next page P - Previous page

Implementierung der Remoteauthentifizierung

Einleitung

Hinweis für CommandCenter-Benutzer

Wenn Sie IP-Reach in die Verwaltungsanwendung CommandCenter von Raritan integrieren und damit steuern möchten, gilt dieser Abschnitt des Benutzerhandbuchs nicht für Sie. Wenn eine IP-Reach-Einheit über CommandCenter gesteuert wird, bestimmt CommandCenter die zulässigen Benutzer und Gruppen. Weitere Informationen finden Sie im CommandCenter-Benutzerhandbuch.

Hinweis für Raritan-Kunden, die vorhergehende Firmwareversionen aktualisieren

Wenn Sie zuvor bereits die RADIUS-Authentifizierung für Raritan-Produkte wie den Dominion KSX und IP-Reach mit älteren Firmwareversionen als Version 3.2 konfiguriert haben, sollten Sie diesen Abschnitt sorgfältig lesen. Beginnend mit Firmwareversion 3.2 wurde die Implementierung der externen Authentifizierung erheblich geändert, um flexiblere und leistungsstärkere Konfigurationen zu ermöglichen.

Unterstützte Protokolle

Zur Vereinfachung der Verwaltung von Benutzernamen und Kennwörtern bietet IP-Reach die Möglichkeit, Authentifizierungsanforderungen an einen externen Authentifizierungsserver weiterzuleiten. IP-Reach unterstützt zwei externe Authentifizierungsprotokolle: LDAP und RADIUS.

Hinweis zu Microsoft Active Directory

Microsoft Active Directory verwendet das LDAP-Protokoll und kann als LDAP-Server und Authentifizierungsquelle für IP-Reach fungieren. Bei Verwendung der IAS-Komponente (Internet-autorisierungsserver) kann ein Microsoft Active Directory-Server auch als RADIUS-Authentifizierungsquelle dienen.

Implementierung der Remoteauthentifizierung

Priorität

Wenn ein Benutzer versucht, sich für eine zur externen Authentifizierung konfigurierte IP-Reach-Einheit zu authentifizieren, durchsucht IP-Reach zunächst seine eigene interne Benutzerdatenbank nach dem Benutzernamen. Ist der Benutzername nicht in der internen Datenbank von IP-Reach enthalten, wird die Anforderung an den externen Authentifizierungsserver weitergeleitet.

- **Wenn der Benutzername nicht in der internen Datenbank von IP-Reach gefunden wird:** Die Anforderung wird an den externen Authentifizierungsserver weitergeleitet, um festzustellen, ob die Anmeldung erlaubt oder verweigert wird.
- **Wenn der Benutzername in der internen Datenbank von IP-Reach gefunden wird und das Kennwort korrekt ist:** Die Anmeldung wird erlaubt.
- **Wenn der Benutzername nicht in der internen Datenbank von IP-Reach gefunden wird und das Kennwort falsch ist:** Die Anmeldung wird verweigert, und die Anforderung wird NICHT an den externen Authentifizierungsserver weitergeleitet.

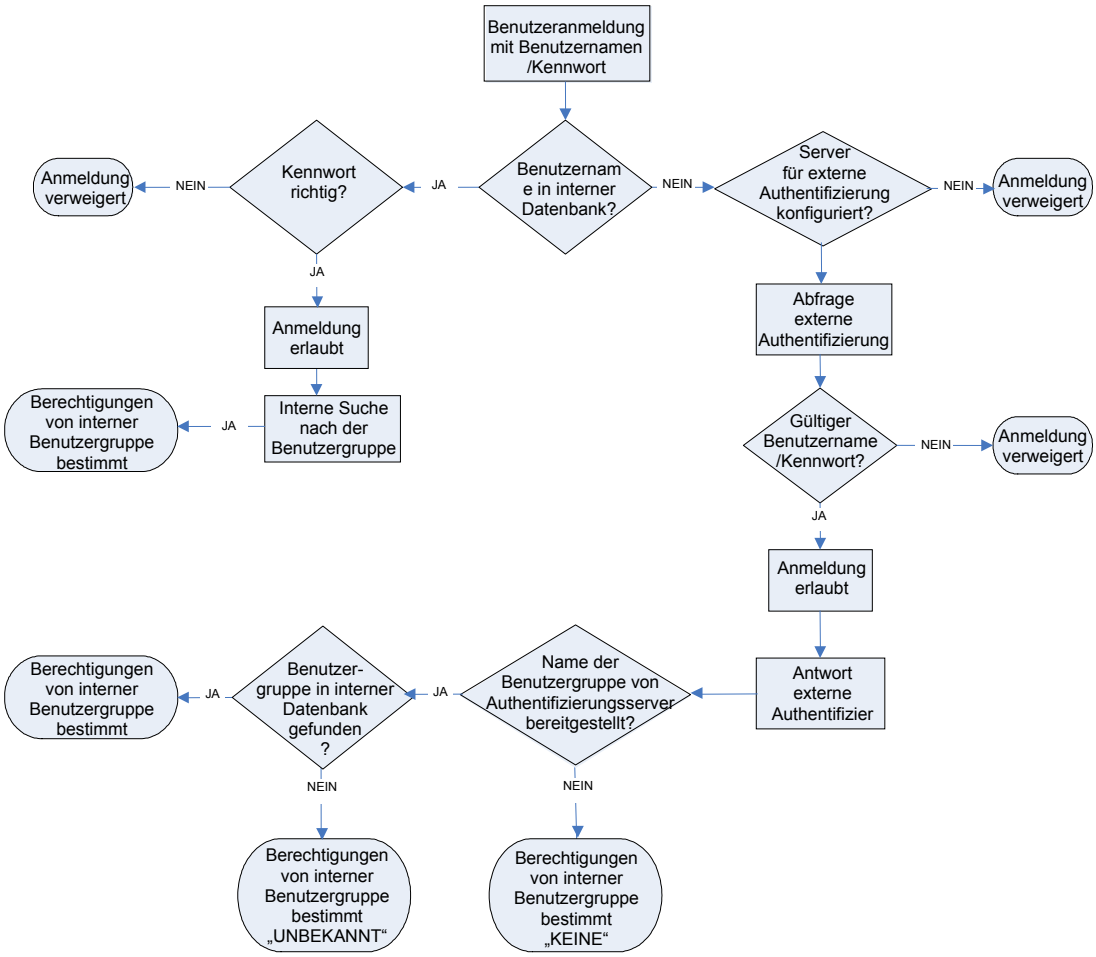
Authentifizierung im Vergleich zur Autorisierung

Wenn Ihre IP-Reach-Einheit zur Remoteauthentifizierung konfiguriert ist, wird der externe Authentifizierungsserver hauptsächlich zur Authentifizierung verwendet und nicht zur Autorisierung.

Die Autorisierung wird von IP-Reach entsprechend der jeweiligen Benutzergruppe festgelegt. Wenn einem Benutzer der Zugriff auf das IP-Reach-System allgemein erlaubt wird (authentifiziert), werden die spezifischen Berechtigungen dieses Benutzers (Autorisierung) folglich entsprechend der Gruppe des Benutzers von IP-Reach bestimmt.

Der externe Authentifizierungsserver kann unterstützend bei der Autorisierung mitwirken, indem er IP-Reach die Benutzergruppe eines Benutzers mitteilt, wenn die Anmeldeanforderung eines Benutzers genehmigt wird. Diese Vorgänge werden in den folgenden Abschnitten **Implementierung der LDAP-Remoteauthentifizierung** und **Implementierung der RADIUS-Remoteauthentifizierung** ausführlicher erläutert.

Das Flussdiagramm unten veranschaulicht die einzelnen Schritte:



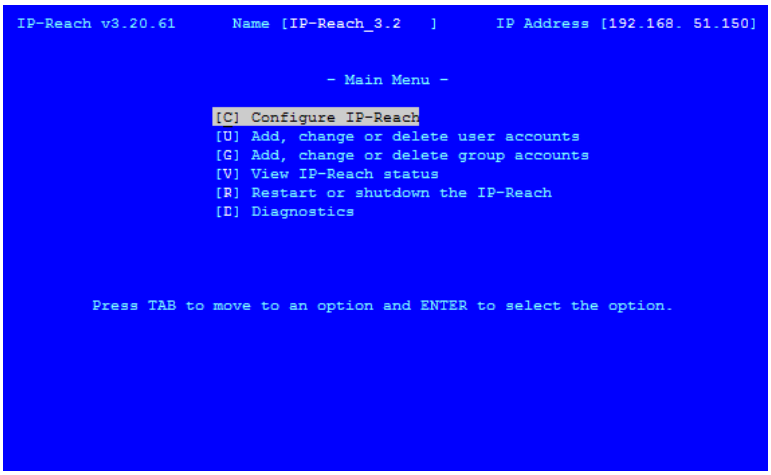
Beachten Sie die Bedeutung der Gruppe, der ein Benutzer angehört, und die Notwendigkeit der Konfiguration der Gruppen UNKNOWN (UNBEKANNT) und NONE (KEINE). Wenn der externe Authentifizierungsserver einen nicht von IP-Reach erkannten Gruppennamen zurückgibt, werden die Berechtigungen dieses Benutzers von der permanenten Gruppe UNKNOWN (UNBEKANNT) bestimmt. Wenn der externe Authentifizierungsserver keinen Gruppennamen zurückgibt, werden die Berechtigungen dieses Benutzers von der permanenten Gruppe NONE (KEINE) festgelegt.

Informationen zur Konfiguration Ihres Authentifizierungsservers, damit dieser bei seiner Antwort auf eine Authentifizierungsanfrage Benutzergruppeninformationen an IP-Reach zurückgibt, finden Sie in den Abschnitten zu **LDAP** und **RADIUS** in diesem Kapitel.

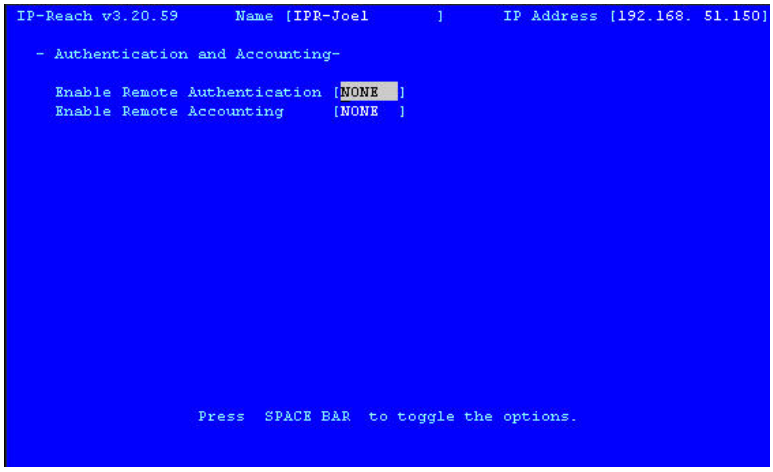
Allgemeine Einstellungen für die Remoteauthentifizierung

Melden Sie sich an IP-Reach als Standardadministrator (Benutzername <admin>, Kennwort <raritan>) an, um die Remoteauthentifizierungseigenschaften festzulegen.

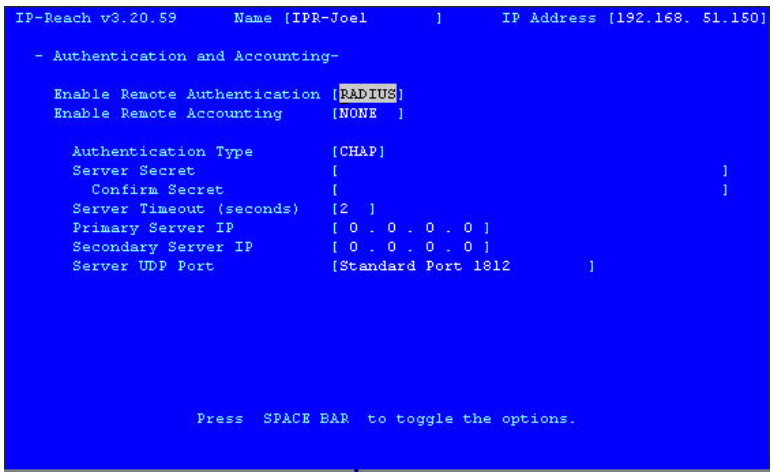
1. Drücken Sie zum Konfigurieren von IP-Reach im Hauptmenü den Buchstaben <**C**>.


IP-Reach v3.20.61 Name [IP-Reach_3.2] IP Address [192.168. 51.150]
- Main Menu -
[C] Configure IP-Reach
[U] Add, change or delete user accounts
[G] Add, change or delete group accounts
[V] View IP-Reach status
[R] Restart or shutdown the IP-Reach
[D] Diagnostics
Press TAB to move to an option and ENTER to select the option.

2. Drücken Sie bei angezeigtem Menü **Configuration** (Konfiguration) den Buchstaben <**R**>, um die Remoteauthentifizierung zu konfigurieren. Das Fenster **Authentication and Accounting** (Authentifizierung und Kontoführung) wird angezeigt.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Authentication and Accounting-
Enable Remote Authentication [NONE]
Enable Remote Accounting [NONE]
Press SPACE BAR to toggle the options.

3. Drücken Sie die LEERTASTE, um zwischen den Optionen für das Remoteauthentifizierungsprotokoll zu wechseln und wählen Sie **RADIUS**, **LDAP** oder **LDAPS**.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Authentication and Accounting-
Enable Remote Authentication [RADIUS]
Enable Remote Accounting [NONE]
Authentication Type [CHAP]
Server Secret [ ]
Confirm Secret [ ]
Server Timeout (seconds) [2]
Primary Server IP [0 . 0 . 0 . 0]
Secondary Server IP [0 . 0 . 0 . 0]
Server UDP Port [Standard Port 1812]
Press SPACE BAR to toggle the options.

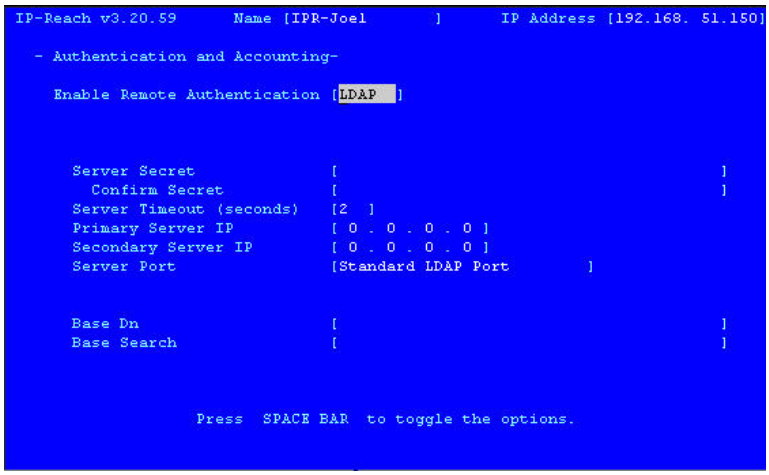
4. Das Fenster **Authentication and Accounting** (Authentifizierung und Kontoführung) für das ausgewählte Protokoll wird angezeigt. Bewegen Sie sich mit der <**TAB**>-Taste durch die Felder.
   a. Drücken Sie die LEERTASTE, um das Feld **Authentication Type** (Authentifizierungstyp) zu aktivieren und zu deaktivieren.

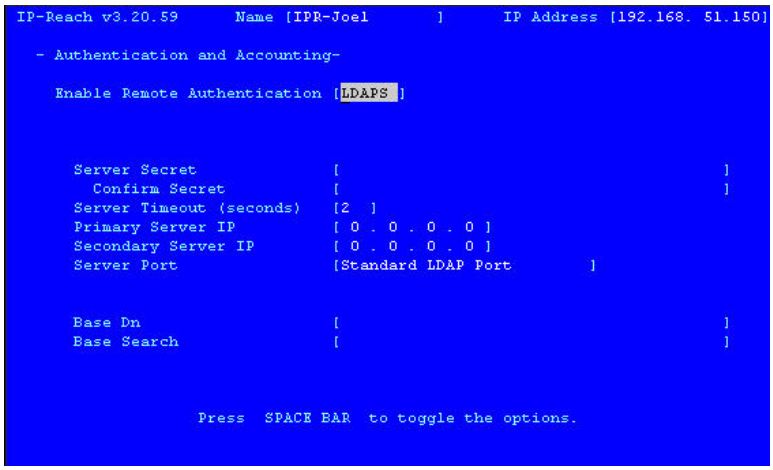
b. Geben Sie den für die Authentifizierung durch die Remoteauthentifizierungsserver erforderlichen geheimen Serverschlüssel in das Feld **Server Secret** (Geheimer Serverschlüssel) ein. Geben Sie den geheimen Serverschlüssel erneut in das Feld **Confirm Secret** (Geheimen Serverschlüssel bestätigen) ein.

c. Geben Sie in das Feld **Server Timeout (seconds)** (Serverzeitüberschreitung [in Sekunden]) die Zeit (in Sekunden) ein, die verstreichen darf, bevor beim Server aufgrund der Inaktivität eine Zeitüberschreitung auftritt.

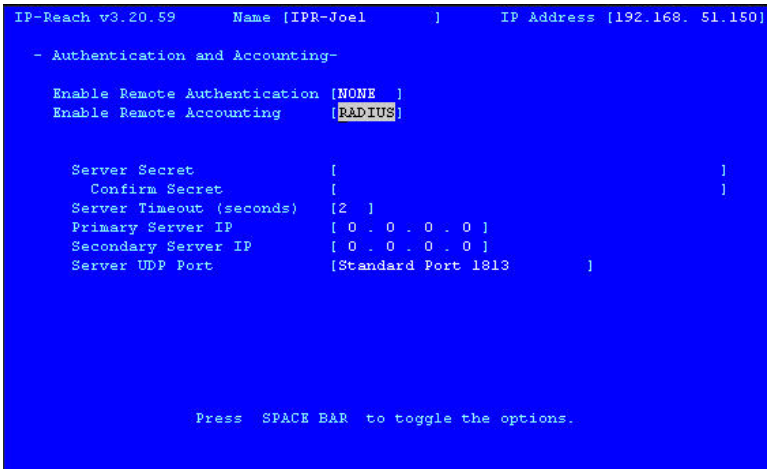
d. Geben Sie in die Felder **Primary Server IP** (IP-Adresse des primären Servers) und **Secondary Server IP** (IP-Adresse des sekundären Servers) die IP-Adressen Ihres primären und sekundären Remoteauthentifizierungsservers ein.

5. Wenn Sie LDAP als Remoteauthentifizierungsprotokoll ausgewählt haben, lesen Sie im folgenden Abschnitt „Implementierung der LDAP-Remoteauthentifizierung“ die Informationen zum Ausfüllen der Felder im LDAP-Bereich des Fensters **Remote Authentication** (Remoteauthentifizierung) nach. Bei Auswahl von RADIUS fahren Sie zum Ausfüllen der Felder im RADIUS-Bereich des Fensters mit dem Abschnitt „Implementierung der RADIUS-Remoteauthentifizierung“ fort.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Authentication and Accounting-
Enable Remote Authentication [LDAP]
Server Secret [ ]
Confirm Secret [ ]
Server Timeout (seconds) [2]
Primary Server IP [0 . 0 . 0 . 0]
Secondary Server IP [0 . 0 . 0 . 0]
Server Port [Standard LDAP Port]
Base Dn [ ]
Base Search [ ]
Press SPACE BAR to toggle the options.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Authentication and Accounting-
Enable Remote Authentication [LDAPS]
Server Secret [ ]
Confirm Secret [ ]
Server Timeout (seconds) [2]
Primary Server IP [0 . 0 . 0 . 0]
Secondary Server IP [0 . 0 . 0 . 0]
Server Port [Standard LDAP Port]
Base Dn [ ]
Base Search [ ]
Press SPACE BAR to toggle the options.

6. Wenn Sie die Remotekontoführung im Fenster **Authentication and Accounting** (Authentifizierung und Kontoführung) aktivieren, springen Sie mit der <**TAB**>-Taste zum Feld **Enable Remote Accounting** (Remotekontoführung aktivieren) und drücken Sie die LEERTASTE, um zu RADIUS zu wechseln.


IP-Reach v3.20.59 Name [IPR-Joel] IP Address [192.168. 51.150]
- Authentication and Accounting-
Enable Remote Authentication [NONE]
Enable Remote Accounting [RADIUS]
Server Secret [ ]
Confirm Secret [ ]
Server Timeout (seconds) [2]
Primary Server IP [0 . 0 . 0 . 0]
Secondary Server IP [0 . 0 . 0 . 0]
Server UDP Port [Standard Port 1813]
Press SPACE BAR to toggle the options.

7. Drücken Sie anschließend zum Speichern Ihrer Änderungen auf die EINGABETASTE, oder drücken Sie <**ESC**>, um das Fenster ohne Speichern der Remoteauthentifizierungskonfigurationen zu schließen.

Implementierung der LDAP-Remoteauthentifizierung

Erinnerung: Microsoft Active Directory fungiert als LDAP-Authentifizierungsserver.

Wenn Sie das LDAP-Authentifizierungsprotokoll ausgewählt haben, füllen Sie die LDAP-Felder folgendermaßen aus:

- **Use Secure LDAP** (Sicheres LDAP verwenden)**:** Verwenden Sie diese Regel, um LDAP-S zu aktivieren. Dadurch wird sichergestellt, dass alle über das Netzwerk übertragenen Authentifizierungsanforderungen und -antworten verschlüsselt werden.
- **Default Port/User Defined Port** (Standardport/Benutzerdefinierter Port)**:** Aktivieren Sie ein Optionsfeld, um festzulegen, ob die standardmäßigen LDAP-TCP-Ports verwendet werden, oder geben Sie Ihren benutzerdefinierten Port an.
- **Base DN, Base Search** und **Certificate File** (Basis-DN, Basissuche und Zertifikatdatei): Fragen Sie den Administrator des Authentifizierungsservers nach den korrekten Werten für diese Felder, um LDAP-Authentifizierungsanfragen von IP-Reach zu verarbeiten.

Rückgabe von Benutzergruppeninformationen über LDAP

Wenn ein LDAP-Authentifizierungsversuch erfolgreich ist, bestimmt IP-Reach die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers. Ihr Remote-LDAP-Server kann diese Benutzergruppennamen bereitstellen, indem er ein wie folgt benanntes Attribut zurückgibt:

```
rciusergroup        attribute type: string
```

Dies erfordert ggf. eine Schemaerweiterung auf Ihrem LDAP-Server. Bitten Sie den Administrator des Authentifizierungsservers, dieses Attribut zu aktivieren.

Implementierung der RADIUS-Remoteauthentifizierung

Microsoft Active Directory kann als Informationsquelle für die RADIUS-Authentifizierung verwendet werden, indem die Windows-Serverkomponente **Internetauthentifizierungsserver** installiert wird.

Wenn Sie das RADIUS-Authentifizierungsprotokoll ausgewählt haben, füllen Sie die RADIUS-Felder folgendermaßen aus:

- **Authentication Type** (Authentifizierungstyp)**:** Klicken Sie auf den Dropdownpfeil, um das CHAP- oder PAP-Protokoll auszuwählen.
- **Server UDP Port/Custom UDP Port** (Server-UDP-Port/Angepasster UDP-Port)**:** Klicken Sie auf den Dropdownpfeil, um festzulegen, ob der standardmäßige RADIUS-TCP-Port 1812 oder der ältere RADIUS-TCP-Port 1645 verwendet werden soll, oder geben Sie Ihren benutzerdefinierten Port in das Feld **Custom UDP Port** (Angepasster UDP-Port) ein.
- **Remote Accounting/Custom Accounting Port** (Remotekontoführung/Angepasster Kontoführungsport)**:** Aktivieren Sie das Kontrollkästchen, um Authentifizierungsereignisse an einen RADIUS-Kontoführungsserver zu senden. Wenn Sie dieses Kontrollkästchen aktivieren, geben Sie den für die Übertragung von Ereignissen zu verwendenden TCP-Port in das Feld **Custom Accounting Port** (Angepasster Kontoführungsport) ein.

Rückgabe von Benutzergruppeninformationen über RADIUS

Wenn ein RADIUS-Authentifizierungsversuch erfolgreich ist, bestimmt IP-Reach die Berechtigungen eines Benutzers anhand der Berechtigungen der Gruppe des Benutzers.

Ihr Remote-RADIUS-Server kann diese Benutzergruppennamen bereitstellen, indem er ein als RADIUS *FILTER-ID* implementiertes Attribut zurückgibt. Die *FILTER-ID* sollte folgendermaßen formatiert werden:

`Raritan:G{GRUPPENNAME}`
Dabei ist `GRUPPENNAME` eine Zeichenfolge, die den Namen der Gruppe angibt, der der Benutzer angehört.

Spezifikationen für den RADIUS-Kommunikationsaustausch

IP-Reach sendet die folgenden Informationen in einer Authentifizierungsanfrage an den RADIUS-Server:

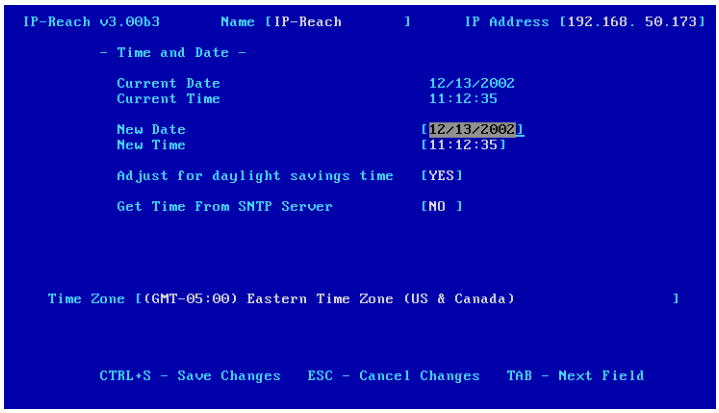
ATTRIBUT	DATEN
USER-NAME	Dies ist der in der Anmeldemaske eingegebene Benutzername.
USER-PASSWORD	Dies ist das im PAP-Modus in der Anmeldemaske eingegebene verschlüsselte Kennwort.
CHAP-PASSWORD	Dies ist die im CHAP-Modus aufgrund des Kennworts und der CHAP-Herausforderungsdaten berechnete CHAP-Protokollantwort.
NAS-IP-ADDRESS	Dies ist die IP-Adresse von IP-Reach.
NAS-IDENTIFIER	Dies ist der im Fenster **Network Configuration** (Netzwerkkonfiguration) konfigurierte Name der IP-Reach-Einheit (siehe hierzu den vorhergehenden Abschnitt).
NAS-PORT-TYPE	Dies ist der Wert ASYNC (0) für Modemverbindungen und der Wert ETHERNET (15) für Netzwerkverbindungen.
NAS-PORT	Dieses Attribut ist immer 0.
STATE	Wenn diese Anforderung als Antwort auf ein ACCESS-CHALLENGE-Ereignis erfolgt, werden die Statusdaten aus dem ACCESS-CHALLENGE-Paket zurückgegeben.
PROXY-STATE	Wenn diese Anforderung als Antwort auf ein ACCESS-CHALLENGE-Ereignis erfolgt, werden die Proxystatusdaten aus dem ACCESS-CHALLENGE-Paket zurückgegeben.

IP-Reach sendet mit jeder Kontoführungsanforderung die folgenden RADIUS-Attribute an den RADIUS-Server:

ATTRIBUT	DATEN
SESSION-TYPE	Dieses Attribut ist entweder START (1) für die Anmeldung oder STOP (2) für die Abmeldung.
SESSION-ID	Dies ist eine Zeichenfolge mit einem eindeutigen Sitzungsnamen. Der Name besitzt das Format „<NAS-IDENTIFIER>:<Benutzer-IP-Adresse>:<eindeutige Sitzungsnummer>“. Beispiel: „IP-Reach:192.168.1.100:122“
USER-NAME	Siehe oben.
NAS-IP-ADDRESS	Siehe oben.
NAS-IDENTIFIER	Siehe oben.
NAS-PORT-TYPE	Siehe oben.
NAS-PORT	Siehe oben.
FILTER-ID	Alle während der Authentifizierung vom RADIUS-Server zurückgegebenen FILTER-ID-Attribute werden in jeder Kontoführungsanforderung gesendet.
CLASS	Alle während der Authentifizierung vom RADIUS-Server zurückgegebenen CLASS-Attribute werden in jeder Kontoführungsanforderung gesendet.
ACCT-AUTHENTIC	Gibt an, wie der Benutzer authentifiziert wurde: entweder RADIUS (1), wenn der Benutzer vom RADIUS-Server authentifiziert wurde, oder LOCAL (2), wenn der Benutzer anhand der internen Benutzernamendatenbank von IP-Reach authentifiziert wurde.
TERMINATE-CAUSE	Wenn dies eine STOP-Anforderung ist, gibt dieses Attribut den Grund für die Beendigung bzw. Trennung des Benutzers an. Der Wert lautet USER_REQUEST (1), LOST_SERVICE (3), SESSION_TIMEOUT (5) oder ADMIN_RESET (6).

Uhrzeit und Datum

In diesem Fenster wird das aktuelle Datum und die Uhrzeit an der IP-Reach-Einheit angegeben. Gespeicherte Änderungen an Uhrzeit und Datum werden erst wirksam, wenn IP-Reach neu gestartet wird.


IP-Reach v3.00b3 Name [IP-Reach] IP Address [192.168. 50.173]
- Time and Date -
Current Date 12/13/2002
Current Time 11:12:35
New Date [12/13/2002]
New Time [11:12:35]
Adjust for daylight savings time [YES]
Get Time From SNTP Server [NO]
Time Zone [(GMT-05:00) Eastern Time Zone (US & Canada)]
CTRL+S - Save Changes ESC - Cancel Changes TAB - Next Field

- **New Date / New Time** (Neues Datum/Neue Uhrzeit)**:** Hier werden Änderungen der aktuellen Datums- und Uhrzeitwerte manuell eingegeben.
- **Adjust for daylight savings time** (Sommerzeitbedingt umstellen)**:** Stellen Sie **YES** (JA) oder **NO** (NEIN) ein, je nachdem ob in Ihrem Land oder Bundesstaat die Sommerzeit gilt.
- **Get Time From SNTP Server** (Zeit vom SNTP-Server abrufen)**:** Gibt an, ob die Uhrzeit bzw. das Datum von IP-Reach automatisch mit der Uhrzeit bzw. dem Datum eines externen SNTP-Servers synchronisiert werden soll.
  - **Primary Server IP Address** (IP-Adresse des primären Servers)**:** Dies ist die IP-Adresse des ersten SNTP-Servers, der die Zeitsynchronisierung vornimmt.
  - **Secondary Server IP Address** (IP-Adresse des sekundären Servers)**:** Dies ist die IP-Adresse des abzufragenden zweiten SNTP-Servers, falls der primäre Server nicht verfügbar ist.
  - **User standard UDP port 123** (Standard-UDP-Benutzerport 123)**:** Ermöglicht Benutzern, den für die SNTP-Zeitsynchronisierung verwendeten UDP-Port zu ändern. Wenden Sie sich an Ihren SNTP-Serveradministrator, um zu erfahren, ob dieser Wert angepasst werden soll.
- **Time Zone** (Zeitzone)**:** Wählen Sie die Zeitzone, in der sich der physische Standort Ihrer IP-Reach-Einheit befindet.

Drücken Sie <**Strg+S**> zum Speichern der Änderungen oder <**Esc**>, um die Änderungen abzubrechen, und kehren Sie zum Menü **Configuration** (Konfiguration) zurück. Gespeicherte Änderungen der RADIUS-Konfiguration werden erst wirksam, wenn IP-Reach neu gestartet wird.

Abmelden von Benutzern

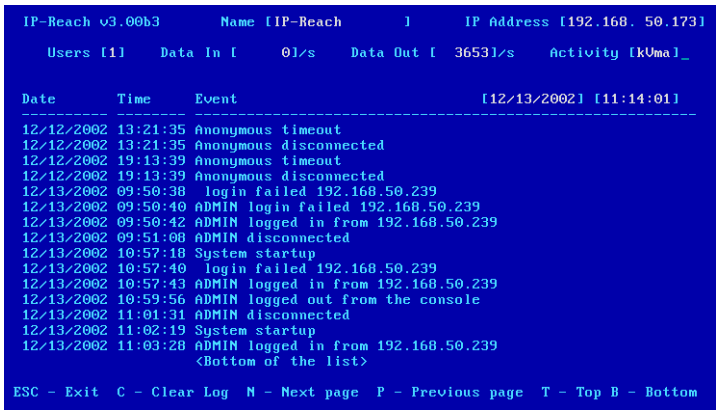
Wählen Sie mit der <**Tab**>-Taste oder den Pfeiltasten <↑> und <↓> einen Benutzer, der zurzeit remote an IP-Reach angemeldet ist ((**Logged in – YES** [Angemeldet – JA]), im Fenster **Add, Change, or Delete User Accounts** (Benutzerkonten hinzufügen, ändern oder löschen) aus, und drücken Sie den Buchstaben <**L**>, um den ausgewählten Benutzer abzumelden. Sie werden gefragt, ob Sie den Benutzer wirklich abmelden möchten.

- **Y:** Ja. Der ausgewählte Benutzer wird von IP-Reach abgemeldet und die Remotesitzung beendet. IP-Reach kehrt zum Fenster **Add, Change, or Delete User Accounts** (Benutzerkonten hinzufügen, ändern oder löschen) zurück. Hier werden alle Benutzerprofile angezeigt, wobei der ausgewählte Benutzer nicht mehr als angemeldet aufgeführt wird.
- **N:** Nein. IP-Reach kehrt zum Fenster **Add, Change, or Delete User Accounts** (Benutzerkonten hinzufügen, ändern oder löschen) zurück. Hier werden alle Benutzerprofile angezeigt, wobei der ausgewählte Benutzer nach wie vor als angemeldet aufgeführt wird.

Anzeigen des IP-Reach-Status

Das IP-Reach-Fenster **Event Log** (Ereignisprotokoll) zeigt eine Protokolldatei mit Informationen über Anmelde- und Verbindungsaktivitäten von IP-Reach an. Dieses Ereignisprotokoll speichert IP-Reach-Ereignisse, z.B. Benutzeran- und -abmeldung, fehlgeschlagene Anmeldeversuche, Admin-Anmeldungen und Abmeldungen von der IP-Reach-Verwaltungskonsole, an der Systemkonfiguration vorgenommene Admin-Änderungen, hinzugefügte, geänderte oder gelöschte Admin-Benutzerprofile, Modemaktivität, Starten und Herunterfahren des Systems und alle aufgetretenen Fehler mit Datum und Uhrzeit für jedes Ereignis. Eine Liste der Fehlercodes mit Bedeutung und Lösungsvorschlag finden Sie in **Anhang D: Problembehandlung**. In einer Protokolldatei können bis zu 2.048 Ereignisse gespeichert werden.

IP-Reach nimmt außerdem eine automatische Wiederherstellung nach schwerwiegenden Fehlern vor. Tritt ein schwerwiegender Fehler auf, wird dieser aufgezeichnet und IP-Reach führt automatisch einen Neustart durch. Wenn ein nicht schwerwiegender Fehler auftritt, wird dieser aufgezeichnet und IP-Reach wartet, bis alle Benutzer vom System abgemeldet sind. Anschließend wird ein Neustart durchgeführt, um sicherzustellen, dass aus dem nicht schwerwiegenden Fehler kein schwerwiegender Fehler wird.


IP-Reach v3.00b3 Name [IP-Reach] IP Address [192.168. 50.173]
Users [1] Data In [0]/s Data Out [3653]/s Activity [kVma]_
Date Time Event [12/13/2002] [11:14:01]
12/12/2002 13:21:35 Anonymous timeout
12/12/2002 13:21:35 Anonymous disconnected
12/12/2002 19:13:39 Anonymous timeout
12/12/2002 19:13:39 Anonymous disconnected
12/13/2002 09:50:38 login failed 192.168.50.239
12/13/2002 09:50:40 ADMIN login failed 192.168.50.239
12/13/2002 09:50:42 ADMIN logged in from 192.168.50.239
12/13/2002 09:51:08 ADMIN disconnected
12/13/2002 10:57:18 System startup
12/13/2002 10:57:40 login failed 192.168.50.239
12/13/2002 10:57:43 ADMIN logged in from 192.168.50.239
12/13/2002 10:59:56 ADMIN logged out from the console
12/13/2002 11:01:31 ADMIN disconnected
12/13/2002 11:02:19 System startup
12/13/2002 11:03:28 ADMIN logged in from 192.168.50.239
<Bottom of the list>
ESC - Exit C - Clear Log N - Next page P - Previous page T - Top B - Bottom

Neustart oder Herunterfahren von IP-Reach

Bietet die Optionen **Restart** (Neustart) <**R**> und **Shutdown** (Herunterfahren) <**S**> sowie **Cancel** (Abbrechen) <**Esc**> zum Abbrechen des Befehls zum Neustart oder Herunterfahren. <**R**> Startet die IP-Reach-Einheit neu und zeigt die Verwaltungskonsole von IP-Reach wieder im IP-Reach-Fenster **Initialization** (Initialisierung) an.

Diagnose

Wenn Sie beim Navigieren im Hauptmenü der Verwaltungskonsole auf **<D>** und die EINGABETASTE drücken, werden die Diagnosefunktionen von IP-Reach aufgerufen.

Diese Funktionen ermöglichen den technischen Kundendienst von Raritan, Sie bei einem Problem mit Ihrer IP-Reach-Einheit zu unterstützen. Rufen Sie diese Funktionen nur auf, wenn Sie sich über deren Bedeutung und den beabsichtigten Zweck im Klaren sind. Weitere Informationen erhalten Sie bei Bedarf vom technischen Kundendienst von Raritan.

-[IP-Reach Diagnostic Console]----------[192.168.050.173]-
V View log LOG Set log mask
<ENTER> View more log M Insert log marker
P Pause Log R Resume log
C Clear the log
NETSTATS Network Statistics PING Send a network ping
RESET Reset to factory defaults RESTART Restarts IP-Reach
Type HELP <commandName> to get more information.
Type X to exit the diagnostic console.
>

Anhang A: Technische Daten

EINSTELLUNG	ABMESSUNGEN BXTXH	GEWICHT	STROMVERSORGUNG
IPR-TR361	2U-19"-Gestellchassis: 482 mm (b) x 540 mm (t) x 89 mm (h) 19" (b) x 21,25" (t) x 3,5" (h)	12,79 kg (28.2 lbs)	110/220V automatische Anpassung (50/60 Hz)
IPR-TR362	2U-19"-Gestellchassis: 482 mm (b) x 540 mm (t) x 89 mm (h) 19" (b) x 21,25" (t) x 3,5" (h)	12,97 kg (28.6 lbs)	110/220V automatische Anpassung (50/60 Hz)
IPR-TR364	2U-19"-Gestellchassis: 482 mm (b) x 540 mm (t) x 89 mm (h) 19" (b) x 21,25" (t) x 3,5" (h)	13,34 kg (29.4 lbs)	110/220V automatische Anpassung (50/60 Hz)
IPR-M1	1U-19"-Gestellchassis: 431 mm (b) x 264 mm (t) x 44 mm (h) 17" (b) x 10,4" (t) x 1,75" (h)	3,8 kg (8.4 lbs)	110/220V automatische Anpassung (50/60 Hz)
IPR-M2	1U-19" -Gestellchassis: 431 mm (b) x 264 mm (t) x 44 mm (h) 17" (b) x 10,4" (t) x 1,75" (h)	3,9 kg (8.6 lbs)	110/220V automatische Anpassung (50/60 Hz)

Remoteverbindung

Netzwerk: 10BASE-T, 100BASE-TX Ethernet
Modem: 56-K-Modem im Lieferumfang enthalten (TR-Serie); Dedizierter Modemport (M-Serie)
Protokolle: TCP/IP, UDP, SNMP

Raritan Remote Client (RRC)-Software

Betriebssystemanforderungen: Windows XP/NT/ME/2000

KVM-Eingabe

Tastatur: PS/2
Maus: PS/2
Video: VGA
Unterstützte Auflösungen:

Textmodi

640x480 bei 60Hz	1024x768 bei 60 Hz
640x480 bei 72Hz	1024x768 bei 70 Hz
640x480 bei 75Hz	1024x768 bei 75 Hz
640x480 bei 85Hz	1024x768 bei 85 Hz
800x600 bei 56 Hz	1152x864 bei 60 Hz
800x600 bei 60 Hz	1152x864 bei 75 Hz
800x600 bei 72 Hz	1280x1024 bei 60 Hz
800x600 bei 75 Hz	
800x600 bei 85 Hz	

Kabelspezifikationen

RJ11-Standardtelefonkabel zur Verbindung von Modem und Telefonleitung (im Lieferumfang enthalten)**

UTP-Kabel der Kategorie 5e zur Verbindung mit dem Netzwerk

**nur TR-Serie

KVM Switch-Spezifikationen

Unterstützt KVM-Switches mit Bildschirmbenutzerschnittstelle, einschließlich der Produktlinien Paragon von Raritan, Z-Serie, MasterConsole MX^4 und MasterConsole II.

Ausgangsspezifikationen

Lokale Zugriffskonsole:	PS/2-Tastatur, PS/2-Maus, HD15-Video
Lokale Verwaltungskonsole:	PS/2-Tastatur, HD15-Video

Anhang B: SNMP-Funktionen

Zur bequemen Überwachung mit Standardnetzwerkverwaltungssystemen wie HP OpenView oder IBM Tivoli-Softwarelösungen, ist IP-Reach mit einem SNMP-Agenten mit MIB2-Standardsupport ausgestattet. IP-Reach antwortet auf SNMP GET-Anfragen mit MIB2-Standardvariablen, wobei allerdings aus Sicherheitsgründen nur eine Teilmenge der Variablen bereitgestellt werden.

Anhang C: Häufig gestellte Fragen

FRAGE:	ANTWORT:
Was ist IP-Reach?	IP-Reach ist die einfachste, schnellste und zuverlässigste Methode für den standortunabhängigen Remotezugriff und die Remoteverwaltung mehrerer mit einem Raritan-KVM-Switch verbundener Server.
Wie funktioniert IP-Reach?	IP-Reach wird mit den Tastatur-, Video- und Mausports eines Servers oder KVM-Switch verbunden. Mit der leistungsfähigen Frame-Grapper- und Komprimierungstechnologie von Raritan erfasst, digitalisiert und komprimiert IP-Reach das Videosignal vor der Übertragung an einen Remote-PC.
Welche Steuerungsmöglichkeiten besitzt ein IP-Reach-Remotebenutzer auf den verbundenen Zielservern?	Der Remotebenutzer verfügt über direkten Zugriff auf die Zielserver und kann diese zur Wartung, Verwaltung und Problembehandlung vollständig steuern. Er kann Anwendungen mit grafischer Benutzeroberfläche ausführen, eine Problembehandlung auf BIOS-Ebene durchführen und sogar Neustarts initiieren.
Remotezugriffssoftware ist seit langem erhältlich. Wie unterscheidet sich IP-Reach von anderen Produkten?	Bei IP-Reach wird die Software nicht auf jedem einzelnen Zielserver ausgeführt, sondern nur auf der IP-Reach-Einheit selbst. Bei herkömmlicher Remotezugriffssoftware muss auf jedem Zielserver Software geladen und ausgeführt werden. Für die Zielserver können daher nur unterstützte Betriebssysteme verwendet werden. Dies kann auf wichtigen Zielservern zu Kompatibilitäts-, Leistungs- und Zuverlässigkeitsproblemen führen.
Welche Methoden der Remotezugriffsverbindung unterstützt IP-Reach?	IP-Reach bietet Netzwerkadministratoren mehrere Methoden für den Remotezugriff: Internet, LAN/WAN und DFÜ-Modem. Dies bedeutet, dass Server sowohl im In-Band- als auch im Out-of-Band-Modus zugänglich sind. Der Remotezugriff auf wichtige Server ist dadurch immer gewährleistet, sogar bei einem Netzwerkausfall.
Welche Computertypen kann IP-Reach remote steuern?	IP-Reach arbeitet unabhängig von der Hardware, dem Betriebssystem oder der Anwendungssoftware der Zielserver und greift auf die Haupteingabe-/-ausgabegeräte (Tastatur, Video, Maus) des Zielservers zu. Daher kann jede Hardware, die standardmäßige PC-Tastaturschnittstellen, standardmäßig PC-Mausschnittstellen und Standard-PC-Video (VGA) unterstützt, zusammen mit IP-Reach verwendet werden.
Ist spezielle Software für den Remote-PC erforderlich?	Jede IP-Reach-Einheit wird mit einer Kopie der IP-Reach Control Software (TRC) ausgeliefert. Diese Remotezugriffssoftware wird auf einem Remote-PC mit dem Betriebssystem Windows 98 oder höher ausgeführt und kommuniziert über das Internet, ein LAN/WAN oder DFÜ-Modem mit der IP-Reach-Software in der IP-Reach-Einheit. Wenn diese Software installiert ist, verhält sich der Remote-PC wie jede andere Benutzerkonsole in Ihrer KVM-Konfiguration, er kann sich jedoch an einem beliebigen Standort befinden – im Nachbarraum oder am anderen Ende der Welt.
Welche Raritan-KVM-Switches können mit IP-Reach eingesetzt werden?	Zurzeit unterstützt Raritan die Verwendung von IP-Reach mit allen Raritan-KVM-Switches, die mit einer Bildschirmanzeige ausgestattet sind: Paragon, MasterConsole MX^4 und MasterConsole II.
Sind andere KVM-Switchmarken mit IP-Reach kompatibel?	Kein anderes Produkt ergänzt IP-Reach besser als ein KVM-Switch von Raritan – insbesondere Paragon. Theoretisch kann IP-Reach jedoch mit jedem beliebigen KVM-Switch eingesetzt werden, der über ein Bildschirmbenutzer-schnittstellenmenü für den Zugriff auf die Switchingfunktionen verfügt.

FRAGE:	ANTWORT:
Kann ich weiterhin lokal auf meine KVM-Konfiguration zugreifen?	Ja. IP-Reach verfügt über einen speziellen direkten analogen Benutzerport für den direkten Zugriff auf die KVM-Konfiguration. Dieser Durchgangsport bietet einen zusätzlichen lokalen Zugriffspunkt, der besonders für Einzelbenutzer-Switches oder den Zugriff auf Server bei einem Netzwerkausfall wichtig ist.
Kann IP-Reach ohne einen KVM-Switch verwendet werden?	Ja. IP-Reach kann für den direkten Zugriff auf einzelne Computer verwendet werden, indem die Einheit an die Tastatur-, Video- und Mausports eines unabhängigen Computers angeschlossen wird. Die Vorteile dieses Produkts kommen jedoch erst durch die Verwendung eines KVM-Switch richtig zum Tragen.
Ist die Installation von IP-Reach einfach?	Die Installation von IP-Reach ist sehr einfach. Schließen Sie die Einheit einfach an einem Benutzerport in einer vorhandenen KVM-Konfiguration an, und weisen Sie ihr eine IP-Adresse und/oder Telefonnummer für den Modemzugriff zu.
Wie wird die IP-Reach-Verwaltung durchgeführt?	Administratoren greifen über eine verbundene IP-Reach-Verwaltungskonsole auf IP-Reach zu. Eine einfache tastaturgesteuerte Schnittstelle mit Menüs ermöglicht die Steuerung und den einfachen Zugriff auf das IP-Reach-Setup. Benutzerprofile, Sicherheitseinstellungen, Konfiguration und Diagnosen sind nur einige der verfügbaren Optionen. Die Verwaltungskonsole von IP-Reach kann aus dem Serverraum entfernt werden, sobald die IP-Reach-Erstkonfiguration abgeschlossen ist. Alle weiteren Konfigurationsvorgänge können remote über einen Webbrowser erfolgen.
Sind Sicherheitsfeatures zum Schutz meiner Zielserver vor nicht autorisierten Remoteverbindungen verfügbar?	Ja. IP-Reach bietet viele Sicherheitsschichten. IP-Reach kann für eine umfassende Verbindungsauthentifizierung und die Sicherheit der Videodatenübertragung während einer Remotesitzung konfiguriert werden. Benutzernamen, Kennwörter, private Schlüssel und 128-Bit-SSL-Verschlüsselung (Secure Socket Layer) sind verfügbar. IP-Reach kann zudem als RADIUS-Client fungieren. Darüber hinaus enthalten alle mit Bildschirmbenutzerschnittstelle ausgestatteten Raritan-KVM-Switches ein vollständiges Sicherheitsschema, das vom Netzwerkadministrator zugewiesene Benutzernamen und Kennwörter für den Zugriff auf Server erfordert.
Kann ich IP-Reach zum Verbessern der Leistung für meine spezifische KVM-Konfiguration anpassen?	Ja. Eine Vielzahl von Anpassungsverfahren sind verfügbar. Die automatische Farbkalibrierung, Anpassung der KVM-Bildschirmanzeige und Einstellungen der Maus auf dem Zielserver dienen zum Verbessern der Leistung von IP-Reach.
Kann ich IP-Reach zum Verbessern der Leistung für unterschiedliche Remotezugriffsmethoden und Situationen anpassen?	Ja. IP-Reach bietet eine Vielzahl von Leistungsanpassungen, die zur Optimierung für eine bestimmte Verbindungsmethode vorgenommen werden können. Farbtiefe, progressive Aktualisierung und Internetflusssteuerung sind nur einige der zum Beschleunigen der Antwortzeit verfügbaren Anpassungsoptionen. Die Farbtiefe kann z.B. komplett von schwarz bis weiß angepasst werden, um die Datenmenge im Fall einer Notfallmodem-verbindung zu wichtigen Servern oder bei niedrigen Bandbreiten zu reduzieren.
Kann ich IP-Reach in einem VPN verwenden?	Ja. IP-Reach lässt sich in nahezu jeder Netzwerkkonfiguration mit Standard-TCP/IP einsetzen. Der Netzwerkadministrator muss IP-Reach lediglich über die IP-Reach-Verwaltungskonsole als Knoten im Netzwerk hinzufügen.
Wie schnell müssen die von IP-Reach unterstützten Verbindungen mindestens sein?	IP-Reach bietet basierend auf der verfügbaren Bandbreite eine skalierbare Leistung. Die niedrigste unterstützte Verbindungsgeschwindigkeit beträgt 20 KBit/s.
Kann ich über eine PBX-Leitung eine DFÜ-Modemverbindung zu IP-Reach herstellen?	Nein. Modems erfordern die Verwendung einer analogen Telefonleitung.

FRAGE:	ANTWORT:
Kann ich IP-Reach in meinem lokalen Netzwerk verwenden?	IP-Reach kann in jedem Computernetzwerk verwendet werden, das TCP/IP unterstützt.
Wann verwendet IP-Reach TCP? Wann verwendet es UDP?	IP-Reach verwendet sowohl TCP als auch UDP. TCP ist jedoch erforderlich, während UDP optional ist. UDP wird nur für eine IP-Reach-Funktion verwendet, und zwar für die automatische Erkennung (**Browse** ([Durchsuchen]) von IP-Reach-Einheiten in einem Subnetz (siehe **Kapitel 3: Raritan Remote Client, *RRC-Navigator***). Wenn Sie die Funktion zum Durchsuchen (und demzufolge DHCP) nicht verwenden, kommuniziert IP-Reach nur über TCP.

Anhang D: Problembehandlung

Probleme und Lösungsvorschläge

REMOTEVERBINDUNGSPROBLEME	LÖSUNG
Ich kann keine Verbindung zu IP-Reach über ein DFÜ-Modem herstellen.	Stellen Sie sicher, dass Sie das Modem für Ihren Remote-PC im Modemfeld **Add Connection Window (Dial-up type connection)** (Verbindungsfenster hinzufügen) [DFÜ-Verbindung]) angegeben haben. Obwohl gleichzeitige Verbindungen aktiviert sein können (entweder global oder individuell), lässt das in IP-Reach integrierte Modem nur eine Remoteverbindung zurzeit zu. Stellen Sie sicher, dass kein anderer Benutzer über Modem mit IP-Reach verbunden ist. Überzeugen Sie sich, dass der Modemzugriff in Ihrem Benutzerprofil aktiviert ist und dass IP-Reach im Fenster **Network Configuration** (Netzwerkkonfiguration) für eine Modemschnittstelle konfiguriert ist. Stellen Sie sicher, dass der vom Netzwerkadministrator im Fenster **Network Configuration** (Netzwerkkonfiguration) ausgewählte Kommunikationsport mit dem in Ihrem Verbindungsprofil festgelegten Port übereinstimmt.
Ich kann keine Verbindung zu IP-Reach über LAN/WAN oder Internet herstellen.	Überprüfen Sie die IP-Einstellungen für IP-Reach von der Verwaltungskonsole von IP-Reach aus oder remote im Fenster **Admin Console** (Verwaltungskonsole). Rufen Sie das Fenster **Network Configuration** (Netzwerkkonfiguration) auf und stellen Sie sicher, dass die für **IP Address** (IP-Adresse), **Subnet Mask** (Subnetzmaske) und **Default Gateway** (Standardgateway) festgelegten IP-Adressen nach Anweisung Ihres Netzwerkadministrators korrekt eingestellt sind. Überzeugen Sie sich, dass der Netzwerkzugriff in Ihrem Benutzerprofil aktiviert ist und dass IP-Reach für eine Netzwerkschnittstelle konfiguriert ist. Stellen Sie sicher, dass der vom Netzwerkadministrator im Fenster **Network Configuration** (Netzwerkkonfiguration) ausgewählte Kommunikationsport mit dem in Ihrem Verbindungsprofil festgelegten Port übereinstimmt. Prüfen Sie, ob die Netzwerkkonfiguration korrekt ist, indem Sie vom Remote-PC einen PING-Befehl an IP-Reach senden.
Ich kann keine Verbindung zu IP-Reach über einen Webbrowser herstellen.	Überprüfen Sie die IP-Einstellungen für IP-Reach von der Verwaltungskonsole von IP-Reach aus oder remote im Fenster **Admin Console** (Verwaltungskonsole). Rufen Sie das Fenster **Network Configuration** (Netzwerkkonfiguration) auf und stellen Sie sicher, dass die für **IP Address** (IP-Adresse), **Subnet Mask** (Subnetzmaske) und **Default Gateway** (Standardgateway) festgelegten IP-Adressen nach Anweisung Ihres Netzwerkadministrators korrekt eingestellt sind. Stellen Sie sicher, dass der Webbrowserzugriff in Ihrem Benutzerprofil aktiviert ist und dass IP-Reach für den Webbrowserzugriff konfiguriert ist.
Ich kann keine Verbindung zu IP-Reach herstellen und scheine im Fenster **Login** (Anmeldung) zu hängen.	Stellen Sie sicher, dass Benutzername und Kennwort gültig und korrekt sind. Überzeugen Sie sich davon, dass Sie Benutzername und Kennwort in genau der gleichen Groß-/Kleinschreibung eingeben, wie sie angelegt wurden. Ziehen Sie das Fenster **Login** (Anmeldung) zur Seite und zeigen Sie das dahinter liegende Fenster **Connection Status** (Verbindungsstatus) an. Im Fenster **Connection Status** (Verbindungsstatus) werden die Einzelheiten Ihrer Verbindungsversuche angezeigt, sodass Sie unter Umständen nähere Informationen zu Ihrem Problem erhalten.

PROBLEME MIT DER DIREKTEN ANALOGEN BENUTZERKONSOLE	LÖSUNG
Die direkte analoge Benutzerkonsole funktioniert nicht.	Stellen Sie sicher, dass der KVM-Switch ordnungsgemäß funktioniert. Überzeugen Sie sich, dass das IP-Reach-Gerät eingeschaltet ist. Das IP-Reach-Gerät muss eingeschaltet sein, damit die direkte analoge Benutzerkonsole funktioniert. Das im IP-Reach-Gerät angebrachte Kabel, das mit dem bzw. die Ports der direkten analogen Benutzerkonsole verbunden ist, ist möglicherweise nicht mehr eingesteckt. Wenden Sie sich an den technischen Kundendienst von Raritan.
Ich bekomme von einer direkten analogen Benutzerkonsole aus keine kontinuierliche Tastatur-/Maussteuerung des aktiven Zielservers.	Die Tastatur-/Maussteuerung eines Zielservers von einer direkten analogen Benutzerkonsole aus wird basierend auf der ersten aktiven Tastatur-/Mauseingabe mit anderen Remotebenutzern, die momentan verbunden sind, gemeinsam verwendet. Stellen Sie sicher, dass zurzeit kein anderer Remotebenutzer versucht, den aktiven Zielserver zu steuern.
Ich kann den gesuchten Zielserver nicht von einer direkten analogen Benutzerkonsole aus anzeigen.	Überzeugen Sie sich, dass Sie mit der direkten analogen Benutzerkonsole arbeiten, die mit dem richtigen Benutzerport verbunden ist. Direkte analaoge Benutzerkonsolen können an die Benutzerports 1 bis 4 angeschlossen werden. Jede Benutzerkonsole zeigt den Pfad des entsprechenden KVM-Ports an. Die mit Benutzerport 1 verbundene Benutzerkonsole zeigt beispielsweise den mit KVM-Port 1 verbundenen KVM-Pfad an. Ebenso zeigt die mit Benutzerport 2 verbundene Benutzerkonsole den mit KVM-Port 2 verbundenen KVM-Pfad an usw.

TASTATURPROBLEME	LÖSUNG
IP-Reach akzeptiert keine Tastaturbefehle vom Remote-PC.	Damit die Tastatursteuerung ordnungsgemäß funktioniert, muss das Fenster **IP-Reach** der IP-Reach Control Software (TRC) aktiv sein. Überzeugen Sie sich davon, dass das Fenster, in dem Sie Eingaben vornehmen, aktiv ist. Versuchen Sie, die Tastatursignale zu löschen, um sicherzustellen, dass das Freigabe- oder Breakcodesignal empfangen wurde. Drücken Sie dazu einige Male die Tasten <**Strg**>, <**UMSCHALT**> und <**TAB**> auf Ihrer Tastatur rasch im Wechsel. Stellen Sie sicher, dass der Remotebenutzer über Tastatur- und Mausberechtigung verfügt. Beenden Sie die IP-Reach-Software und starten Sie sie anschließend neu.
Ich habe die Feststelltaste an meinem Remote-PC gedrückt. Auf der Statusleiste von IP-Reach wird die Anzeige für Großbuchstaben angezeigt, doch die Feststellanzeige auf der Tastatur meines Remote-PCs leuchtet nicht.	Das ist normal. Bestimmen Sie den Status der Feststelltaste für den Zielserver anhand der Anzeigen auf der Statusleiste. Wenn ein lokaler Benutzer an der Tastatur der direkten analogen Benutzerkonsole den Status der Feststelltaste (Feststelltaste, Num-Feststelltaste und Rollen-Taste) auf dem Zielserver geändert hat, stimmt der Status des Servers unter Umständen nicht mit dem Status der Tastatur des Remote-PCs überein.
Die Tastatur funktioniert nicht und die grüne LED-Anzeige auf der Rückseite des IP-Reach-Geräts blinkt bei mindestens einem KVM-Port nicht auf, leuchtet ständig.	Setzen Sie die Tastaturchips im IP-Reach-Gerät durch Ein- und Ausschalten zurück. Achten Sie darauf, sowohl das IP-Reach-Gerät sowie alle verbundenen KVM-Switches gleichzeitig auszuschalten. Anderenfalls werden die KVM-Chips im IP-Reach-Gerät über die KVM-Switches mit Strom versorgt und werden nicht zurückgesetzt.
Beim Zugriff auf IP-Reach über den Webbrowser funktioniert die Tastatur nicht. Beim Drücken der Tasten passiert nichts.	Klicken Sie auf die Fenstertitelleiste unter der IP-Reach-Symbolleiste, um das Anzeigefenster zu aktivieren. Die Tastatur funktioniert nur, wenn das Anzeigefenster aktiv ist.

PROBLEME MIT DER KVM-BILDSCHIRMBENUTZERSCHNITTSTELLE	LÖSUNG
Durch Klicken auf die Schaltfläche **Enter On-Screen Menu** (Bildschirmmenü öffnen) wird die Bildschirmbenutzerschnittstelle des verbundenen KVM-Switch nicht aufgerufen. Es passiert nichts.	IP-Reach ist möglicherweise nicht für die richtige Zugriffstastenaktivierung des KVM-Switch eingerichtet. Die Standardeinstellung für die Zugriffstaste ist <Rollentaste> oder **Rollentaste+Rollentaste** im IP-Reach-Fenster **Options** (Optionen). Stellen Sie sicher, dass die im Fenster **Options** (Optionen) festgelegte Zugriffstaste mit der Zugriffstaste übereinstimmt, die die Bildschirmbenutzerschnittstelle des mit IP-Reach verbundenen KVM-Basisswitch steuert. Wählen Sie im Menü des Fensters **IP-Reach** die Optionen **Tools** → **Options** (Extras → Optionen). Das Fenster **Options** (Optionen) wird geöffnet. Wählen Sie die entsprechende Zugriffstaste, die die Bildschirmbenutzerschnittstelle des verbundenen KVM-Switches aktiviert. **Rollentaste +Rollentaste** = <Rollentaste>, **Num-Festelltaste+Num-Feststelltaste** = <Num-Feststelltaste> und **Feststelltaste +Feststelltaste** = <Feststelltaste>. Klicken Sie zum Fortfahren auf **OK**.
Mit meinem Remote-PC ist ein KVM-Switch verbunden. Durch Eingeben von <Rollentaste> <Rollentaste> (oder einer anderen zugewiesenen Zugriffstaste für die Bildschirmbenutzerschnittstelle des KVM-Switch) von der Tastatur des Remote-PCs aus werden zwei Bildschirmbenutzerschnittstellen aktiviert, und zwar eine für den mit meinem Remote-PC verbundenen KVM-Switch und eine für den mit IP-Reach verbundenen KVM-Basisswitch.	Beenden Sie durch einmaliges Drücken der Taste <**Esc**> auf der Benutzerkonsole des Remote-PCs die Bildschirmbenutzerschnittstelle für den KVM-Switch des Remote-PCs. Nach einigen Sekunden wird die Bildschirmbenutzerschnittstelle für den KVM-Switch des Remote-PCs nicht mehr angezeigt. Um dieses Problem zu vermeiden, können Sie entweder den mit dem Remote-PC verbundenen KVM-Switch auf eine Zugriffstaste zurücksetzen, die sich von der Zugriffstaste für den mit IP-Reach verbundenen KVM-Basisswitch unterscheidet. Oder aktivieren Sie die Bildschirmbenutzerschnittstelle für den mit IP-Reach verbundenen KVM-Basisswitch nur über IP-Reach-Befehle. Klicken Sie dazu auf die Schaltfläche **Enter On-Screen Menu** (Bildschirmmenü öffnen).
Im Fenster **Security Configuration** (Sicherheitskonfiguration) ist die Abmeldung von KVM beim Trennen der Verbindung auf **YES** (JA) eingestellt, doch IP-Reach meldet sich nach der Trennung eines Remote-benutzers nicht von KVM ab.	Stellen Sie sicher, dass die im Fenster **Options** (Optionen) festgelegte Zugriffstaste mit der Zugriffstaste übereinstimmt, die die Bildschirmbenutzerschnittstelle des mit IP-Reach verbundenen KVM-Basisswitch steuert.

MAUSPROBLEME	LÖSUNGEN
Der **Cursor des Zielservers** folgt dem **IP-Reach-Cursor** zu langsam. Unmittelbar nach der Umstellung auf einen neuen Channel des Zielservers hält die Maus an und/oder ist nicht mehr synchron.	Bei der Arbeit mit einem Remote-PC ist eine leichte Verzögerung zwischen dem größeren **IP-Reach-Cursor** und dem kleineren **Cursor des Zielservers** in der Regel aufgrund von nicht steuerbaren Verzögerungen bei der Geschwindigkeit der Remoteverbindung (Internet, DFÜ-Modem oder Netzwerk) normal. Bei jedem neuen Videobild, das angezeigt wird, synchronisiert und richtet IP-Reach die Cursor neu aus. Warten Sie einige Sekunde nach dem Umstellen auf ein neues Videobild, bis die automatische Neukalibrierung stattgefunden hat und die beiden Cursor wieder synchron arbeiten. Wenn Sie die automatische Kalibrierung nicht abwarten möchten und die beiden Cursor auch in anderen Fällen nicht synchron sind, klicken Sie auf **Synchronize Mouse** (Maus synchronisieren) oder drücken Sie die Tasten <**Strg-Alt-S**> gleichzeitig. Mit diesem Befehl werden die beiden Cursor manuell neu ausgerichtet.

MAUSPROBLEME	LÖSUNGEN
	Passen Sie die Bewegung des **Cursors des Zielservers** an. Stellen Sie bei Zielservern mit Windows 2000 die Mausgeschwindigkeit auf die mittlere Geschwindigkeitseinstellung ein und setzen Sie die Mausbeschleunigung für jeden Zielserver auf <off> (aus) oder <none> (keine). Stellen Sie die Mausgeschwindigkeit für Zielserver mit Windows 95, 98 und NT für jeden Zielserver auf die langsamste Geschwindigkeit ein. Die Farbeinstellungen sind nicht optimal kalibriert. Führen Sie die automatische Farbkalibrierung aus (siehe **Kapitel 3: Raritan Remote Client, *Farbkalibrierung)***.
Der größere **IP-Reach-Cursor** folgt dem kleineren **Cursor des Zielservers** nicht bzw. beide sind nicht synchron (nicht aufeinander ausgerichtet).	Klicken Sie auf **Synchronize Mouse** (Maus synchronisieren) oder drücken Sie <Strg-Alt-S>. Stellen Sie sicher, dass jeder Zielserver einen Windows-Standardmaustreiber verwendet. Stellen Sie bei Zielservern mit Windows 2000 die Mausgeschwindigkeit auf die mittlere Geschwindigkeitseinstellung ein und setzen Sie die Mausbeschleunigung für jeden Zielserver auf <none> (keine). Stellen Sie die Mausgeschwindigkeit für Zielserver mit Windows 95, 98 und NT für jeden Zielserver auf die langsamste Geschwindigkeit ein. Klicken Sie auf **Auto-sense Video** (Video automatisch erkennen) oder drücken Sie gleichzeitig <Strg-Alt-A>.
IP-Reach akzeptiert meine Maus nicht.	IP-Reach unterstützt keine serielle Maus oder Maustreiber, die nicht dem Standard entsprechen. Es unterstützt eine PS/2-Maus und Standard-Windows-Maustreiber. Andere Maustreiber funktionieren unter Umständen mit IP-Reach auch, erfordern jedoch umfangreiche Änderungen der Mauseinstellungen, bis eine entsprechend funktionierende Mischung von Bewegungseinstellungen gefunden wird. Wenn Sie einen Maustreiber auf einem Zielserver verwenden müssen, der von IP-Reach zurzeit nicht unterstützt wird, stellen Sie die Mausbeschleunigung auf <none> (keine) und die Mausgeschwindigkeit auf <slow> (langsam) ein.
Der IP-Reach-Cursor und der Cursor des Zielservers werden in einigen Verwaltungsfenstern von Windows NT, wie der Windows NT-Anmeldemaske, nicht synchronisiert.	Verwaltungsfenster oder Anmeldemasken von Windows NT werden möglicherweise auf Standardeinstellungen für die Cursorbewegegung/-beschleunigung zurückgesetzt. In diesen Masken ist die Maussynchronisierung daher nicht optimal. Wenn Sie sich mit der Anpassung der Registrierung von Windows NT-Zielservern auskennen, können Sie in den NT-Anmeldemasken eine bessere IP-Reach-Maussynchronisierung erzielen, indem Sie den Registrierungs-Editor des Zielservers aufrufen und folgende Einstellungen ändern: default user mouse motion speed = 0; mouse threshold 1= 0; mouse threshold 2 = 0.

PROBLEME MIT DEM ZIELSERVER	LÖSUNG
Wenn ich einen Zielserver von einem Remote-PC aus über IP-Reach neu starte, kann ich nicht auf das BIOS des Zielservers zugreifen. IP-Reach akzeptiert anscheinend den Befehlstastaturanschlag des BIOS-Eintrags nicht.	Für den Zugriff auf das BIOS eines Zielservers deaktivieren Sie vorübergehend das Kontrollkästchen **Sense video mode changes automatically** (Videomodusänderungen automatisch erkennen) im Fenster **Video Settings** (Videoeinstellungen), das Sie durch Klicken auf **Video Settings** (Videoeinstellungen) auf der IP-Reach-Symbolleiste öffnen. Durch die automatische Videoerkennung wird die Remoteanzeige des

	Neustartvorgangs verlangsamt. Dadurch wird das Senden von BIOS-Zugriffstastaturanschlägen an den Zielserver von einem Remote-PC erschwert, da die automatische Erkennung IP-Reach anweist, kontinuierlich mit den sich rasch ändernden Videofenstern während des Neustarts des Zielservers Schritt zu halten. Durch Deaktivieren des Kontrollkästchen für die automatische Erkennung wird IP-Reach in die Lage versetzt, BIOS-Zugriffstastaturanschläge zu akzeptieren und zu übertragen. Außerdem wird so die schnelle Interpretation der sich rasch ändernden Videofenster unterstützt. Stellen Sie sicher, dass Sie das Kontrollkästchen erneut aktivieren, wenn Sie den BIOS-Zugriff beendet haben.

PROBLEME MIT IP-REACH	LÖSUNG
Es ist keine Steuerung und keine Bildabtasteraktivität vorhanden. IP-Reach scheint gesperrt zu sein.	Möglicherweise hat sich ein internes serielles Datenkabel, das die Bildabtasterkarte mit der Hauptplatine von IP-Reach verbindet, gelöst. Wenden Sie sich an den technischen Support von Raritan.
Ich kann IP-Reach nicht ausschalten.	Der Hauptnetzschalter für IP-Reach befindet sich auf der Rückseite des Geräts. Um IP-Reach auszuschalten, halten Sie den Netzschalter einige Sekunden lang gedrückt. Um IP-Reach wieder einzuschalten, drücken Sie erneut den Netzschalter.
Nach einem Stromausfall schaltet sich IP-Reach nicht automatisch wieder an.	Rufen Sie das BIOS von IP-Reach auf und stellen Sie sicher, dass **Power Lost Resume State** (Bei Stromausfall Zustand wiederherstellen) auf **Last State** (Letzter Zustand) eingestellt ist. IP-Reach schaltet sich dann bei wiederhergestellter Stromversorgung nur wieder ein, wenn das Gerät bereits eingeschaltet war, bevor der Stromausfall auftrat.

VIDEOPROBLEME	LÖSUNG
Nach der Umstellung auf einen anderen Channel des Zielservers ist die Videoanzeige nicht klar. Mitunter weist der Bildschirm des Zielservers einen schwarzen Rand auf.	Klicken Sie auf **Auto-sense Video** (Video automatisch erkennen) oder drücken Sie gleichzeitig die Tasten <Strg-Alt-A>. IP-Reach passt daraufhin die Videoeinstellungen an. Wenn die Videoanzeige nicht klar wird, sind möglicherweise weitere manuelle Anpassungen der Videoeinstellungen erforderlich. Wenden Sie sich an den technischen Kundendienst von Raritan, um Änderungen im Fenster **Video Settings** (Videoeinstellungen) zu besprechen. Stellen Sie sicher, dass alle Zielserver Standard-deaktivierungszeiten aufweisen. Horizontale und vertikale Deaktivierungszeiten sollten in etwa VESA-Standardwerten entsprechen.
Bei der Remoteanzeige eines Zielservers enthält das Videobild einen sich bewegenden Block mit falscher Farbe, der der Bewegung des Cursors zu folgen scheint.	Die Farbeinstellungen auf der Registerkarte **Video Settings** (Videoeinstellungen) im Fenster **Video** sind nicht richtig eingestellt. Passen Sie die Einstellungen manuell an, bis die Blockierung der Farbe aufgehoben wird, oder führen Sie die automatische Farbkalibrierung aus (siehe **Kapitel 3: Raritan Remote Client, *Farbkalibrierung)***.

VIDEOPROBLEME	LÖSUNG
Der Bildschirm enthält kleine visuelle Fehler oder fehlende Farbkörnung, die bereinigt werden muss.	Klicken Sie auf der IP-Reach-Symbolleiste auf **Refresh Screen** (Bildschirm aktualisieren) oder drücken Sie die Tasten <**Strg-Alt-R**> gleichzeitig.
Die Videoanzeige scheint im automatischen Erkennungsmodus hängen geblieben zu sein und die automatische Erkennungsmeldung in der Mitte des Bildschirms zählt immer weiter.	Durch Drücken von **Auto-sense Video** (Video automatisch erkennen), während die automatische Erkennung ausgeführt wird, wird der automatische Erkennungsvorgang angehalten. Prüfen Sie die Auflösung Ihres Zielservers, um sicherzustellen, dass diese von IP-Reach unterstützt wird.

PROBLEME MIT DEM WEBBROWSER	LÖSUNG
Ich kann keine Verbindung zu IP-Reach über einen Webbrowser herstellen.	Überprüfen Sie die IP-Einstellungen für IP-Reach von der Verwaltungskonsole von IP-Reach aus oder remote im Fenster **Admin Console** (Verwaltungskonsole). Rufen Sie das Fenster **Network Configuration** (Netzwerkkonfiguration) auf und stellen Sie sicher, dass die für **IP Address** (IP-Adresse), **Subnet Mask** (Subnetzmaske) und **Default Gateway** (Standardgateway) festgelegten IP-Adressen nach Anweisung Ihres Netzwerkadministrators korrekt eingestellt sind. Stellen Sie sicher, dass der Webbrowserzugriff in Ihrem Benutzerprofil aktiviert ist und dass IP-Reach für den Webbrowserzugriff konfiguriert ist.

Ereignisprotokolldatei und Bildschirmfehlercodes

Sobald ein Problem auftritt, zeigt IP-Reach einen Fehlercode an oder protokolliert diesen im Fenster **IP-Reach Event Log** (IP-Reach-Ereignisprotokoll). Fehlercodes sind achtstellige Hexadezimalzahlen, die aus zwei Teilen bestehen: Die ersten vier Zahlen bezeichnen den Fehlertyp und die letzten vier enthalten einen Standortcode.

Diese letzten vier Zahlen des IP-Reach-Fehlercodes sind äußerst nützlich, um die Ursache für einen Systemausfall zu bestimmen. In der nachstehenden Tabelle sind Standortcodes aufgeführt (d.h. die letzten vier Zahlen eines Fehlercodes) sowie die entsprechende Bedeutung.

FEHLERCODE (DIE LETZTEN 4 ZAHLEN)	BEDEUTUNG	EMPFEHLUNG
0001 – 0003	Speicherzuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0004	Die Konfigurationsdatei konnte beim Start nicht gelesen werden. Die Datei oder das Dateisystem ist beschädigt oder die Konfigurationsdatei wurde mit einer älteren Version von IP-Reach erstellt.	Geben Sie die erforderlichen Konfigurationsinformationen erneut ein und starten Sie IP-Reach neu. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.

FEHLERCODE (DIE LETZTEN 4 ZAHLEN)	BEDEUTUNG	EMPFEHLUNG
0005	Die Konfigurationsdatei ist nicht vorhanden. Entweder starten Sie IP-Reach zum ersten Mal, oder das Dateisystem ist beschädigt.	Geben Sie die erforderlichen Konfigurations-informationen erneut ein und starten Sie IP-Reach neu. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0006	Die Konfigurationsdatei konnte nicht gespeichert werden. Das Dateisystem ist beschädigt oder die Festplatte reagiert nicht.	Versuchen Sie es erneut. Falls das Problem jedoch weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0007 – 0008	Speicherzuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
Löschen	Speicherzuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0009	Die Bildabtasterkarte konnte nicht gefunden werden.	Schalten Sie das System aus und vergewissern Sie sich, dass die Bildabtasterkarte ordnungsgemäß eingesteckt wurde. Falls das Problem weiterhin besteht, könnte dies auf ein Problem mit der IP-Reach-Hardware hindeuten.
000A	Die Bildabtasterkarte reagiert nicht ordnungsgemäß.	Schalten Sie das System aus und vergewissern Sie sich, dass die Bildabtasterkarte ordnungsgemäß eingesteckt wurde. Falls das Problem weiterhin besteht, könnte dies auf ein Problem mit der IP-Reach-Hardware hindeuten.
000B	Speicherzuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
000C – 000F	Speicherzuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0011	Der Ethernet-Controller konnte nicht gefunden werden.	Es besteht ein Problem mit der IP-Reach-Hardware.
0012	Das Modem konnte nicht gefunden werden.	Schalten Sie das System aus und vergewissern Sie sich, dass die Bildabtasterkarte ordnungsgemäß eingesteckt wurde. Falls das Problem weiterhin besteht, könnte dies auf ein Problem mit der IP-Reach-Hardware hindeuten.
0013	Speicherzuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0014	Bei der IP-Adresse ist ein Fehler aufgetreten.	Prüfen Sie die Konfiguration der IP-Adresse und starten Sie das System neu.

FEHLERCODE (DIE LETZTEN 4 ZAHLEN)	BEDEUTUNG	EMPFEHLUNG
0015	Der DHCP-Server reagiert nicht. IP-Reach konnte keine IP-Adresse abrufen.	Stellen Sie sicher, dass der DHCP-Server ordnungsgemäß funktioniert, und starten Sie IP-Reach neu.
0016 – 0019	Bei einer der IP-Reach-Startdateien ist ein Fehler aufgetreten.	Stellen Sie die Software und das Dateisystem anhand der Recovery-CD-ROM wieder her.
001A	Beim Initialisieren des UDP-Sockets ist ein Fehler aufgetreten.	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
001B	Beim Initialisieren des TCP-Schreibsockets ist ein Fehler aufgetreten.	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
001C	Beim Initialisieren des TCP-Lesesockets ist ein Fehler aufgetreten.	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
001D – 001E	Ressourcen-zuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
001F	Der TCP-Schreibsocket konnte nicht abgehört werden.	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0020	Der TCP-Lesesocket konnte nicht abgehört werden.	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0021	Fehler beim TCP-Abhörvorgang	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0022	Fehler beim UDP-Abhörvorgang	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0023	Fehler beim SSL-Schreibvorgang	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0024	Fehler beim SSL-Lesevorgang	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.

FEHLERCODE (DIE LETZTEN 4 ZAHLEN)	BEDEUTUNG	EMPFEHLUNG
0025	Speicherzuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0026 – 0029	Ressourcen-zuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
002A – 002F	Ressourcen-zuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0030-0039	Ressourcen-zuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
003A – 003F	Ressourcen-zuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.
0040	Ressourcen-zuweisungsfehler	Starten Sie IP-Reach neu. Vergewissern Sie sich, dass der BIOS-Speichertest mindestens 64 MB RAM erkennt. Falls das Problem weiterhin besteht, stellen Sie die Software und das Dateisystem von der Recovery-CD-ROM wieder her.